Good towers of function Fields

Nguyen, Nhut

Publication date:
2015

Document Version
Publisher's PDF, also known as Version of record

Good towers of function fields

Nhut Nguyen

PhD-2015-394

Technical University of Denmark
Department of Applied Mathematics and Computer Science
Richard Petersens Plads, Building 324,
DK-2800 Kongens Lyngby, Denmark
Phone: +45 4525 3031
Email: compute@compute.dtu.dk
Hompage: www.compute.dtu.dk

Summary

Algebraic curves are used in many different areas, including error-correcting codes. In such applications, it is important that the algebraic curve C meets some requirements. The curve must be defined over a finite field $\mathbb{F}_q$ with q elements, and then the curve also should have many points over this field. There are limits on how many points $N(C)$ an algebraic curve C defined over a finite field can have. An invariant of the curve which is important in this context is the curve's genus $g(C)$. Hasse and Weil proved that $N(C) \leq q + 1 + 2\sqrt{q}g(C)$ and this bound can in general not be improved. However if the genus is large compared with q, the bound can be improved. Drinfeld and Vladut showed the asymptotic result:

$$A(q) := \limsup_{g(C)\to\infty} \frac{N(C)}{g(C)} \leq \sqrt{q} - 1.$$

The quantity $A(q)$ is called Ihara's constant. If q is a square, it is known that $A(q) = \sqrt{q} - 1$, while the value of the $A(q)$ is unknown for all other values of q.

In this thesis, we study a construction using Drinfeld modules that produces explicitly defined families of algebraic curves that asymptotically achieve Ihara's constant. Such families of curves can also be described using towers of function fields. Restated in this language the aim of the project is to find good and optimal towers. Using the theory of Drinfeld modules and computer algebraic techniques, some new examples of

good towers are obtained. We analyse towers of Drinfeld modular curves describing certain equivalence classes of rank 2 Drinfeld modules. Using rank 3 Drinfeld modules further examples of good towers are produced.

Resumé

Algebraisk kurver anvendes i forskellige områder, blandt andet fejlrettende koder. I sådanne anvendelser er det vigtigt at den algebraiske kurve C opfylder nogle krav. Kurven skal være defineret over et såkaldt endeligt legeme $\mathbb{F}_q$ med q elementer, og så skal kurven også have så mange punkter som muligt over dette endelige legeme. Der er dog grænser på hvor mange punkter $N(C)$ en algebraisk kurve C defineret over et endeligt legeme kan have. En invariant af kurven som er vigtigt i denne sammenhæng er kurvens genus $g(C)$. Hasse og Weil har vist at $N(C) \leq q + 1 + 2\sqrt{q}\, g(C)$ og denne grænse kan generelt ikke forbedres. Men hvis genus bliver stort i forhold til q, kan grænsen forbedres og Drinfeld og Vladut har vist det asymptotiske resultat:

$$A(q) := \limsup_{g(C)\to\infty} \frac{N(C)}{g(C)} \leq \sqrt{q} - 1.$$

Konstanten $A(q)$ kaldes for Ihara's konstant. Hvis q er et kvadrat, vides at $A(q) = \sqrt{q} - 1$, mens værdien af $A(q)$ er ukendt for alle andre værdier af q.

I denne afhandling undersøges en konstruktion vha. Drinfeld moduler som producerer eksplicit beskrevne familier af algebraiske kurver som asymptotisk opnår Ihara's konstant. Sådanne familier af kurver kan også beskrives som tårne af funktionslegemer. Omformuleret til dette sprog handler projektet om at find gode og optimale tårne. Vha. teorien af

Drinfeld moduler samt komputer algebraiske tekniker, angives en del nye eksempler af gode tårner. Der analyseres også tårne af Drinfeld modulære kurver som beskriver visse ækvivalensklasser af rang 2 Drinfeld moduler. Ved brug af rang 3 Drinfeld moduler produceres nogle eksempler, samt nogle tårne som er beslægtet ved teori af rang 3 Drinfeld moduler, undersøges.

Preface

This dissertation is submitted for the degree of Doctor of Philosophy at Technical University of Denmark. The research was conducted under the supervision of Professor Peter Beelen at the Department of Applied Mathematics and Computer Science between August 2012 and October 2015. This work is written in manuscript-style. It contains the three following articles.

[BBN14] A. Bassa, P. Beelen and N. Nguyen, Good towers of function fields, in *Algebraic curves and finite fields*, volume 16 of *Radon Ser. Comput. Appl. Math.*, pages 23–40, De Gruyter, Berlin, 2014.

[BBN15] A. Bassa, P. Beelen and N. Nguyen, *Good families of Drinfeld modular curves*, LMS Journal of Computation and Mathematics **18**, 699–712 (2015).

[ABNed] N. Anbar, P. Beelen and N. Nguyen, The exact limit of some cubic towers, in *Arithmetic, geometry, cryptography and coding theory (AGCT 2015)*, submitted.

Kongens Lyngby, November 2015.
Nhut Nguyen

Acknowledgements

First and foremost, I would like to thank Peter Beelen for the guidance and the support that he provided me during my Ph.D. study. Peter taught me how to choose problems to work on, helped me solve them and explained me every simple thing. Without Peter's mentoring, contagious enthusiasm and endless support, my Ph.D. study and this thesis would not have been possible. Having Peter as my advisor was a truly unique experience that I will always remember. I learned a great deal from it.

I also want to thank Nurdagül Anbar for her help and support during the time I was in İstanbul in the Winter 2013-2014 and later when she joined our group at DTU Compute in November 2014. Also with Nurdagül's very careful corrections, our publications and my thesis were completed with very few errors.

I am grateful to Tom Høholdt and his Danish–Chinese Project on Applications of Algebraic Geometry in Coding Theory and Cryptography. He and his project gave me a great opportunity to do a Ph.D. in Denmark.

It is a pleasure to be a co-author with Alp Bassa for the first two publications. Thanks to Alp, Nurdagül and Sabancı Üniversitesi for hosting my visit in Turkey. For the times visiting there, I would like to thank Otto Mønsted Fond for supporting my travels and stays.

The change from the old DTU Mathematics to the new Section of Mathematics did not affect the atmosphere and activities. I have very nice colleagues in building 303B. I would like to thank our section's secretary Dorthe Thøgersen for her help on paper work and her readiness to help. Special thanks to Johan Sebastian Rosenkilde Nielsen for always giving me helpful tips and useful information for my career. Thanks to Adnan Banci for being a nice office mate. Thanks to Peter Nørtoft and the football club, thanks to Vu Hong Linh and the badminton club; you are very nice guys.

Finally, I am immensely grateful to my wife Thanh-Thuy and my girls Mai-Khanh and Khanh-Chi for an unbelievable amount of support, love, and happiness that they have given me during my study in Denmark. This thesis is dedicated to them.

Contents

Chapter 1

Introduction

Given a polynomial $f(X_1, ..., X_n) \in \mathbb{Z}[X_1, ..., X_n]$, the question of how many solutions $(x_1, ..., x_n) \in \mathbb{Z}^n$ the Diophantine equation $f(x_1, ..., x_n) = 0$ can have, has been a central and important one in the history of mathematics. For example, consider the equation

$$a^n + b^n = c^n,$$

where a, b, and c are positive integers. When $n = 2$, there are infinitely many solutions. Such a solution (a, b, c) is called a Pythagorean triple, describing the three integer-side lengths of a right triangle. There are several elementary proofs for the solutions and interesting stories around this problem. For $n > 2$ Fermat's Last Theorem stated in 1637 that there is no solution for this equation. The theorem challenged mathematicians more than 350 years until A. Wiles gave a correct proof in 1995. Along with the beautiful proofs and elegant results, many branches of mathematics appeared from such a simple question, from classical number theory to modern algebra and algebraic geometry. Nowadays we find applications of algebra and number theory frequently in our daily life. This thesis deals with such a question in the area of algebraic curves over finite fields.

1.1 What is a good tower of function fields?

Let K be a field and C be an algebraic curve over K. In this thesis we assume that such a curve C is absolutely irreducible, nonsingular and projective. For detailed definitions and facts on algebraic curves we refer to for example [Ful]. A point whose coordinates belong to K is called K-*rational* (or *rational*). If K has infinite elements, the number of rational points of C might be infinite, but for applications in for example coding theory and cryptography one usually considers algebraic curves defined over a finite field. In that case, the number $N(C)$ of K-rational points is always finite. Such a curve C defined over a finite field K has two important invariants: its genus $g(C)$ and its number $N(C)$ of K-rational points. The question of how many rational points a curve C of genus $g(C)$ defined over a finite field can have, has been a central and important one in number theory. One of the landmark results in the theory of curves defined over finite fields was the theorem of Hasse and Weil, which is the congruence function field analogue of the Riemann hypothesis. As an immediate consequence of this theorem one obtains an upper bound for the number of rational points of such a curve in terms of its genus and the cardinality of the finite field. More precisely the Hasse–Weil inequality states that, for a curve C defined over the finite field $\mathbb{F}_q$ with q elements, one has

$$N(C) \leq q + 1 + 2g(C)\sqrt{q}.$$

For interesting applications, one would like to consider algebraic curves defined over a fixed finite field with $N(C)$ as large as possible. The Hasse–Weil bound is not optimal when the genus $g(C)$ is large compared with the cardinality of the finite field. In order to investigate the asymptotic behaviour of the number of rational points $N(C)$ compared to the genus $g(C)$, one is interested in *Ihara's constant*

$$A(q) := \limsup_{g(C)\to\infty} \frac{N(C)}{g(C)},$$

where C runs over all algebraic curves over $\mathbb{F}_q$. By Hasse–Weil bound, $A(q) \leq 2\sqrt{q}$. This was improved by Drinfeld and Vladut [VD83] that $A(q) \leq \sqrt{q} - 1$ over any finite field $\mathbb{F}_q$. On the other hand, Ihara [Iha81], Tsfasman, Vladut and Zink [TVZ82] used modular curves to show that $A(q) \geq \sqrt{q} - 1$ for square q. As a result it is known that $A(q) = \sqrt{q} - 1$ if q is square, unknown otherwise.

To investigate the quantity $A(q)$, it is natural to consider families $\mathcal{F}/\mathbb{F}_q = (C_0, C_1, ...)$ of algebraic curves over $\mathbb{F}_q$ with genus tending to infinity. As there exists a one-to-one correspondence between algebraic function fields and non-singular irreducible projective curves, many geometric concepts can be transferred to the algebraic context and vice versa (see [Ful]). In this thesis, we will stay in the domain of algebraic function fields. We will investigate **towers of function fields** $\mathcal{F}/\mathbb{F}_q = (C_0, C_1, ...)$ with full constant field $\mathbb{F}_q$.

One of the most important measure of the 'quality' of such a family $\mathcal{F}/\mathbb{F}_q$ is its *limit* $\lambda(\mathcal{F}/\mathbb{F}_q)$ which is defined by

$$\lambda(\mathcal{F}/\mathbb{F}_q) := \lim_{i\to\infty} \frac{N(C_i)}{g(C_i)}.$$

One can see that $0 \leq \lambda(\mathcal{F}/\mathbb{F}_q) \leq A(q)$. Then a non-trivial lower bound for Ihara's constant $A(q)$ can be obtained by a family $\mathcal{F}/\mathbb{F}_q$ with positive limit. Such a family $\mathcal{F}/\mathbb{F}_q$ with positive limit is called ***good***. Moreover if $\lambda(\mathcal{F}/\mathbb{F}_q) = A(q)$, the tower $\mathcal{F}/\mathbb{F}_q$ is called *optimal*.

1.2 How to construct good towers?

In [Iha81] Ihara used Shimura curves to show that $A(q) \geq \sqrt{q} - 1$ for square q. About the same time and independently, Tsfasman, Vladut and Zink [TVZ82] used elliptic modular curves and Shimura curves to show that $A(q) \geq \sqrt{q} - 1$ for $q = p^2$ and $q = p^4$ where p is a prime number. However, these curves are in general not easy to describe by explicit equations. Another approach due to Serre [Ser83] uses class field theory in order to prove the existence of curves of arbitrary high genus with sufficiently many rational points, which shows $A(q) > 0$. Also this construction is not explicit. The concept of **explicit towers** was first introduced by Garcia and Stichtenoth [GS95] and [GS96b]. For example, the optimal tower in [GS96b] was defined as a sequence of function fields $(F_i)_{i\geq 0}$ over $\mathbb{F}_{q^2}$ such that $F_0 = \mathbb{F}_{q^2}(x_0)$ and $F_{i+1} = F_i(x_{i+1})$ where

$$x_{i+1}^q + x_{i+1} = \frac{x_i^q}{x_i^{q-1} + 1} \text{ for } i \geq 0.$$

Because of its recursive construction, we say that the tower is recursive and satisfies the recursive equation

$$Y^q + Y = \frac{X^q}{X^{q-1}+1}.$$

An example over a cubic finite field is the tower of van der Geer and van der Vlugt [vdGvdV02] which was defined recursively by

$$Y^2 + Y = X + 1 + \frac{1}{X}.$$

This tower over $\mathbb{F}_8$ has limit $3/2$. Another example of a tower over cubic finite fields is the one of Bezerra, Garcia and Stichtenoth [BGS05b] which was defined recursively by

$$\frac{1-Y}{Y^q} = \frac{X^q + X - 1}{X}.$$

This tower over $\mathbb{F}_{q^3}$ has limit $2(q^2-1)/(q+2)$. Up to present, many explicit good and optimal towers have been introduced. A big breakthrough in the area of towers of function fields is the one given by Bassa, Beelen, Garcia and Stichtenoth [BBGS15]. They introduced a tower $\mathcal{F}/\mathbb{F}_{q^n}$ for any $n \geq 2$ and recursively defined by

$$\mathrm{Tr}_j\left(\frac{Y}{X^{q^{n-j}}}\right) + \mathrm{Tr}_{n-j}\left(\frac{Y^{q^j}}{X}\right) = 1, \tag{1.1}$$

where $n > j > 0$ with $\gcd(j,n) = 1$ and $\mathrm{Tr}_a(T) := T + T^q + \cdots + T^{q^{a-1}}$ for any $a \in \mathbb{N}$. The tower's limit satisfies

$$\lambda(\mathcal{F}/q^n) \geq 2\left(\frac{1}{q^{n-j}-1} + \frac{1}{q^j - 1}\right)^{-1}.$$

Problems: It is not clear how one can find such explicit equations in order to construct good towers as the ones given above. Moreover, computing the limits for those towers requires complicated and technical calculations.

One way is using computer for searching good candidates. In [LMSE02] a non-deterministic algorithm was performed to search for explicit equations that recursively define asymptotically good tame towers over some

small characteristics. Essentially, the algorithm checks if the ramification locus is finite and the splitting locus is not empty. The algorithm in [LMSE02] was refined in [MW05] by putting more sufficient conditions for the construction and providing new techniques for the implementation. The idea of using computer search for construction towers with different defining equations were proposed in [LÖ7] and graph theory was used to study the ramification and the splitting structure.

Various new tame towers have been then exhibited by computer search. Generally, tame towers have the advantage that the genus computation is simple. In [GSR03], by studying the asymptotic behaviour of the number of rational places in tame towers, Garcia, Stichtenoth and Rück produced several good towers of Fermat type and of quadratic extensions. In [BB05] Beelen and Bouw explained the optimal tower in [GSR03] by considering the Picard–Fuchs differential equations in characteristic p and applied their study to towers of modular curves to find new asymptotically good towers.

In this thesis we deal with the **Problems** using the theory of Drinfeld modular curves. In [Elk98, Elk01] Elkies used the theory of classical, Shimura and Drinfeld modular curves to produce explicit optimal towers. Moreover, he observed that the optimal towers constructed by Garcia and Stichtenoth [GS95, GS96a, GS96b, GST97] all arose from reductions of elliptic modular curves, Shimura modular curves, or Drinfeld modular curves. Based on these examples, he predicted that all optimal towers arise from reductions of such kinds of modular curves, known as the Elkies' modularity conjecture (see [Elk98, 'Fantasia']). In [Gek04] Gekeler showed that any (elliptic or Drinfeld) modular curves of Hecke type are optimal.

One of the key strengths of using Drinfeld modules is that it looks promising to construct good towers over any non-prime finite field $\mathbb{F}_{q^n}$ with $n \geq 2$. An example of using Drinfeld modules of rank n to construct good towers over any non-prime finite field $\mathbb{F}_{q^n}$ is the recent work of Bassa, Beelen, Garcia and Stichtenoth [BBGS15]. As a Drinfeld modular explanation for their new tower (defined by Equation (1.1)), a subtower was

addressed and satisfied a recursive equation

$$\frac{(Y+1)^{N_n}}{Y^{N_j}} = \frac{(X+1)^{N_n}}{X^{q^{n-j}N_j}} \ , \tag{1.2}$$

where $n > j > 0$ with $\gcd(j, n) = 1$ and $N_j = (q^j - 1)/(q - 1)$ for $j \geq 1$.

Situation: For all these constructions based on the theory of Drinfeld modular curves mentioned above, the simplest case of Drinfeld A-modules is considered, namely when the base ring A is the polynomial ring $\mathbb{F}_q[T]$ and the fixed place ∞ of the function field $\mathbb{F}_q(T)$ of the ring $\mathbb{F}_q[T]$ has degree $\delta = 1$.

Challenge: One can ask if the situation can be extended to other base rings A and other values of δ.

The most important contribution of this thesis is to give an exploration of this challenge.

1.3 Our contributions

This thesis is written in manuscript style. Chapters 3, 4 and 5 consist of three articles which have been written and submitted during the Ph.D. study. The articles corresponding to Chapter 3 and Chapter 4 have appeared. The one from Chapter 5 is under review. They share a certain background and references, therefore some modifications were made in those chapters compared to the published versions to avoid overlap.

Chapter 2 gives the general background for the articles which appear in subsequent chapters. We start with an overview on the number of rational places of a function field over a finite field. Then definitions and basic properties of towers of function fields are introduced. A definition and properties of Drinfeld modules are briefly given, especially the notion of a Drinfeld modular curve is introduced as the main tool for the explicit construction of the towers. Some examples are given to illustrate definitions and facts. Specially, Example 2.20 presents the idea of how

to obtain a modular relation similar to Equation (1.2) from isogenous Drinfeld modules to define recursive towers.

In **Chapter 3** we elaborate further the ideas of Elkies in [Elk98] and [Elk01]. We show how the defining equations for the towers can be read off from the modular polynomial. To illustrate this, we work out the equations for a few cases of Drinfeld modular towers over the ring $A = \mathbb{F}_q[T]$. Propositions 3.1 and 3.3 will explain how a Drinfeld modular curve corresponds to such a relation like Equation (1.2). In the last section of the chapter, we study a variation where the ring A is replaced by the coordinate ring of an elliptic curve with 5 points. We illustrate the ideas by going through this specific example in detail. As a result, a tower with limit at least 1 over $\mathbb{F}_{2^{10}}$ will be introduced.

Chapter 4 deals with the theory of Drinfeld modular curves over any possible base ring A and values of δ. We write down an explicit formula for the genus of the Drinfeld modular curve $x_0(\mathfrak{n})$ (see Theorem 4.2) and investigate the number of rational points on its reduction (see Theorem 4.4). Consequently, a lower bound for the limit of (reductions of) Drinfeld modular towers $(x_0(\mathfrak{n}_k))_k$ is proved (see Theorem 4.5). It turns out that good reductions of Drinfeld modular towers are always good, when defined over a proper constant field, but not always optimal. We also give a recursive description of such towers in Section 4.4. The theory presented in this chapter fully explains the behaviour of a Drinfeld modular tower given in the last section of Chapter 3. Furthermore, an explicit recursive description of an optimal Drinfeld tower over $\mathbb{F}_{2^8}$ that has not been considered in the literature before is given in Section 4.5. This further demonstrates that explicit descriptions of Drinfeld modular towers are not restricted to the case that the base ring A is the polynomial ring $\mathbb{F}_q[T]$.

In **Chapter 5**, we compute the exact limit of the tower in [BBGS15] when it is defined over cubic finite fields. To do this, we examine the subtower satisfying Equation (1.2). We will prove that the tower's limit equals $2(q^2-1)/(q+2)$ and discuss the relationship between several towers.

Chapter 6 discusses some further developments and future work.

The **Appendix A** presents the Magma computations supporting Section 4.5.

Chapter 2

Background

This chapter gives the general background. More technical and topic-focused preliminaries can be found in the articles which appear in the later chapters. Through out this thesis we denote by $\mathbb{F}_q$ the finite field of cardinality q and by p the characteristic of $\mathbb{F}_q$. We are interested in function fields over $\mathbb{F}_q$ having many rational places with respect to its genus. In this chapter we give some background on towers of function fields and Drinfeld modules, from which good towers can be obtained explicitly. For basic concepts and facts about algebraic function fields (such as the definitions of function fields, places, divisors, rational places, genus, ramification, the Riemann-Roch theorem, the Hurwitz genus formula, etc.) and towers we refer to Stichtenoth's book [Sti09] and his survey article [GS07], about Drinfeld modules we refer to Goss' book [Gos96].

2.1 Rational places of function fields

2.1.1 Function fields and places

Let K be any field. An *algebraic function field F of one variable over K*, denoted by F/K, is a finite algebraic extension of the rational function field $K(x)$ for some element $x \in F$ which is transcendental over K. Such a function field F/K can be obtained as $F = K(x, y)$ by adjoining a root y of an irreducible polynomial in $K(x)[T]$ to $K(x)$.

The set $\tilde{K}$ of elements in F which are algebraic over K is called the *field of constants* of F/K. If $K = \tilde{K}$ we say that K is algebraically closed in F or K is the *full constant field* of F.

A *valuation ring* of a function field F/K is a ring $\mathcal{O} \subseteq F$ such that $K \subsetneq \mathcal{O} \subsetneq F$ and if $z \in F$ then either $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$. A valuation ring of a function field is a local ring; i.e., it has a unique maximal ideal.

A *place* P of a function field F/K is the maximal ideal of a valuation ring $\mathcal{O}$ of F/K. Then the residue class ring $\mathcal{O}/P$ is a field, denoted by F_P. Moreover, F_P is a finite vector space over K, whose dimension $\dim_K F_P$ is called the *degree* of the place P, denoted by $\deg P$. The set of places of F is denoted by $\mathbb{P}_F$. A place of degree one is called *rational*.

Example 2.1 (Rational function field)**.** The simplest algebraic function field over K is the rational function field $F = K(x)$, where x is transcendental over K. Given an irreducible monic polynomial $p(x) \in K[x]$, then

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x] \text{ and } p(x) \nmid g(x) \right\}$$

is a valuation ring of $K(x)/K$ with maximal ideal

$$P_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) | f(x) \text{ and } p(x) \nmid g(x) \right\}.$$

The residue class field $\mathcal{O}_{p(x)}/P_{p(x)}$ is isomorphic to $K[x]/(p(x))$ and $\deg P_{p(x)} = \deg p(x)$. There is another valuation ring of $K(x)/K$, namely

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x] \text{ and } \deg f(x) \leq \deg g(x) \right\}$$

with the maximal ideal

$$P_\infty := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \deg f(x) < \deg g(x) \right\}.$$

Rational places of $K(x)/K$ consist of places of type $P_{x-\alpha}$ with $\alpha \in K$ and P_∞. We also denote by $(x = \alpha)$ the place $P_{x-\alpha}$, the *zero* of $x - \alpha$, and by $(x = \infty)$ the place P_∞, the *pole* of x.

2.1.2 Ihara's constant $A(q)$

We are interested in function fields over a finite field; i.e., K is some finite field $\mathbb{F}_q$. Let F be a function field with full constant field $\mathbb{F}_q$. Assume that the L-polynomial of F factors as

$$L(t) = \prod_{i=1}^{2g(F)} (1 - \alpha_i t),$$

where α_i are complex numbers. Then

$$N(F) = q + 1 - \sum_{i=1}^{2g(F)} \alpha_i.$$

The Hasse–Weil theorem states that $|\alpha_i| = \sqrt{q}$ for all $i = 1, ..., 2g(F)$. Therefore $N(F)$ is bounded in terms of $g(F)$ and q by

$$N(F) \leq q + 1 + 2g(F)\sqrt{q}. \tag{2.1}$$

See [Sti09, Chapter 5] for more detailed proofs. Ihara showed in [Iha81] that if $N(F)$ reaches this upper bound then $g(F)$ can not exceed $(q - \sqrt{q})/2$. If we fix the finite field, in order to get function fields with large $N(F)$, the genus $g(F)$ has to be large also. This leads us to investigate the asymptotic behaviour of the ratio $N(F)/g(F)$ for function fields of large genus. For this reason, Ihara introduced the quantity

$$A(q) := \limsup_{g(F)\to\infty} \frac{N(F)}{g(F)},$$

where F runs over all function fields over $\mathbb{F}_q$. The quantity $A(q)$ plays an important role in coding theory and cryptography. For example, by

using algebraic geometry codes [Gop81] on curves defined over $\mathbb{F}_q$, one can get the *Algebraic Geometry Code bound* [TVZ82]

$$R + \delta \geq 1 - A(q)^{-1},$$

where $R = k/n$ is the transmission rate and $\delta = d/n$ is the relative minimum distance of the code with length $n \to \infty$.

By Hasse–Weil bound (2.1), $A(q) \leq 2\sqrt{q}$. This was improved by Drinfeld and Vladut [VD83] that

$$A(q) \leq \sqrt{q} - 1 \text{ over any finite field } \mathbb{F}_q.$$

On the other hand, Ihara [Iha79], Tsfasman, Vladut and Zink [TVZ82] used modular curves to show that $A(q) \geq \sqrt{q} - 1$ for square q. As a result it is known that

$$A(q) = \sqrt{q} - 1 \text{ if } q \text{ is square.}$$

In particular, for squares $q \geq 49$ the Algebraic Geometry Code bound gives us

$$R + \delta \geq 1 - \frac{1}{\sqrt{q} - 1},$$

which is better than the Gilbert–Varshamov bound in a certain interval (see [TVZ82]).

The exact value of $A(q)$ is still an open question for non-square q. There are some lower bounds for $A(q)$. By using class field theory, Serre [Ser83] showed that there exists a constant $c > 0$ such that $A(q) > c \cdot \log q$ for all q. Zink [Zin85] using degenerations of Shimura curves showed that

$$A(p^3) \geq 2(p^2 - 1)/(p + 2),$$

for p prime. The Zink bound was generalized to any prime power q by Bezerra, Garcia and Stichtenoth [BGS05b] as

$$A(q^3) \geq 2(q^2 - 1)/(q + 2). \tag{2.2}$$

Recently, it was shown [BBGS15] by explicit construction that for $q = p^n$ where p is prime and $n > 1$,

$$A(p^n) \geq 2 \left(\frac{1}{p^{\lceil n/2 \rceil} - 1} + \frac{1}{p^{\lfloor n/2 \rfloor} - 1} \right)^{-1}. \tag{2.3}$$

In particular when n is even, one retrieves the result by Ihara, Tsfasman, Vladut and Zink. And for $n = 3$ one obtains Zink's bound.

2.2 Towers of function fields

To give a good lower bounds for $A(q)$ one is naturally led to towers of function fields.

Definition 2.2. A *tower* over $\mathbb{F}_q$ is an infinite sequence $\mathcal{F} = (F_0, F_1, \cdots)$ of function fields such that for all $i \geq 0$ we have $1 < [F_{i+1} : F_i] < \infty$, F_{i+1}/F_i is separable, $\mathbb{F}_q$ is the full constant field of F_i and the genera $g(F_i) \to \infty$ for $i \to \infty$.

Proposition 2.3. *Let $\mathcal{F} = (F_0, F_1, \cdots)$ be a tower over $\mathbb{F}_q$. For a fixed integer $j \geq 0$, the following limits exist:*

$$\nu(\mathcal{F}/F_j) := \lim_{n\to\infty} \frac{N(F_n)}{[F_n : F_j]} \text{ and } \gamma(\mathcal{F}/F_j) := \lim_{n\to\infty} \frac{g(F_n)}{[F_n : F_j]}.$$

Proof. (see [Sti09, Lemma 7.2.3]). □

The quantities $\nu(\mathcal{F}/F_j)$ and $\gamma(\mathcal{F}/F_j)$ are called *the splitting rate* and *the genus of the tower $\mathcal{F}$ over F_j*, respectively. One has that

$$0 \leq \nu(\mathcal{F}/F_j) \leq N(F_j) \text{ and } 0 < \gamma(\mathcal{F}/F_j) \leq \infty \text{ for } j \geq 0.$$

Then the following limit exists

$$\lambda(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)},$$

since it equals $\nu(\mathcal{F}/F_j)/\gamma(\mathcal{F}/F_j)$ for any $j \geq 0$. The quantity $\lambda(\mathcal{F})$ is called *the limit* of the tower $\mathcal{F}$.

By definition of $\lambda(\mathcal{F})$ and $A(q)$ one gets $0 \leq \lambda(\mathcal{F}) \leq A(q)$. A tower $\mathcal{F}$ over $\mathbb{F}_q$ is called *(asymptotically) good* if $\lambda(\mathcal{F}) > 0$, otherwise it is called *(asymptotically) bad*. A good tower with $\lambda(\mathcal{F}) = A(q)$ is called *(asymptotically) optimal*. One can see that if for some $j \geq 0$, the genus $\gamma(\mathcal{F}/F_j)$ is finite and the splitting rate $\nu(\mathcal{F}/F_j)$ is strictly positive, then the tower $\mathcal{F}$ is good. In order to study the genus and the splitting rate of a tower, it is often sufficient to investigate the notions of ramification locus and splitting locus.

Definition 2.4. Let $\mathcal{F} = (F_0, F_1, \cdots)$ be a tower over $\mathbb{F}_q$ and P be a place of F_j for some integer $j \geq 0$.

- We say that P is *ramified in the tower* $\mathcal{F}$ if for some $n > j$ there exists a place Q of F_n lying above P such that $Q|P$ is *ramified*; i.e., the ramification index satisfies $e(Q|P) > 1$. The set of places of F_j ramified in $\mathcal{F}$ is called the *ramification locus of* $\mathcal{F}$ *over* F_j, denoted by $\mathrm{Ram}(\mathcal{F}/F_j)$.

- Assume that P is a rational place. We say that P *splits completely in the tower* $\mathcal{F}$ if P *splits completely* in all extensions F_n/F_j for $n > j$; i.e., there are exactly $[F_n : F_j]$ places of F_n above the place P and they are rational places of F_n. The set of rational places of F_j splitting completely in $\mathcal{F}$ is called the *splitting locus of* $\mathcal{F}$ *over* F_j, denoted by $\mathrm{Split}(\mathcal{F}/F_j)$.

The splitting locus is a finite set which maybe empty. The ramification locus maybe finite or infinite. The following proposition gives us some ingredients to get good towers.

Proposition 2.5. *[Sti09, Theorem 7.2.10] Let $\mathcal{F} = (F_0, F_1, \cdots)$ be a tower over $\mathbb{F}_q$ and j be a fixed non-negative integer. Then the following holds*

(i) The splitting rate satisfies $\nu(\mathcal{F}/F_j) \geq |\mathrm{Split}(\mathcal{F}/F_j)|$.

(ii) Assume that the ramification locus $\mathrm{Ram}(\mathcal{F}/F_j)$ is finite and that for each place P in $\mathrm{Ram}(\mathcal{F}/F_j)$ there exists a real number b_P such that for all $n > j$ and for all places Q of F_n lying above P, the different exponent $d(Q|P)$ is bounded by

$$d(Q|P) \leq b_P \cdot e(Q|P).$$

Then the genus $\gamma(\mathcal{F}/F_j)$ is finite and

$$\gamma(\mathcal{F}/F_j) \geq g(F_j) - 1 + \frac{1}{2} \sum_{P \in \mathrm{Ram}(\mathcal{F}/F_j)} b_P \cdot \deg P.$$

(iii) Now we assume that the splitting locus $\mathrm{Split}(\mathcal{F}/F_j)$ *is non-empty and that Tower* $\mathcal{F}$ *satisfies conditions in item* (ii)*. Then the tower* $\mathcal{F}$ *is asymptotically good, and its limit satisfies*

$$\lambda(\mathcal{F}) \geq \frac{2|\ \mathrm{Split}(\mathcal{F}/F_j)|}{2g(F_j) - 2 + \sum_{P \in \mathrm{Ram}(\mathcal{F}/F_j)} b_P \cdot \deg P} > 0.$$

Let $b := \max\{b_P \mid P \in \mathrm{Ram}(\mathcal{F}/F_j)\}$*, then the tower* $\mathcal{F}$ *is called* b*-bounded.*

Good towers which appear in the literature are of the following three types:

1. class field towers (see among others [Ser83, NX01]),
2. modular towers (see among others [Iha81, Elk98, Elk01, TVZ82]), and
3. explicit towers (see among others [GS95, GS96b, GSR03, BGS05b]).

By an *explicit tower* we mean a tower $\mathcal{F} = (F_0, F_1, \cdots)$ where each function field F_i is given by explicit polynomial equations. For practical applications in coding theory and cryptography one needs an explicit description of the underlying function fields and of their $\mathbb{F}_q$-rational places. Here we will mainly deal with explicit towers. Even more, the explicit description of the function fields $F_0, F_1, ...$ in the tower $\mathcal{F}$ will often have the following very simple shape.

Definition 2.6. Let $\mathcal{F} = (F_0, F_1, \cdots)$ be a tower of function fields over $\mathbb{F}_q$, where $F_0 = \mathbb{F}_q(x_0)$ is the rational function field. We say that the tower $\mathcal{F}$ is *recursive* if there exist a polynomial $f(X, Y) \in \mathbb{F}_q[X, Y]$ and functions $x_n \in F_n$ such that:

(i) $f(X, Y)$ is separable in both variables X and Y;

(ii) $F_{n+1} = F_n(x_{n+1})$ with $f(x_n, x_{n+1}) = 0$ for all $n \geq 0$.

We also say that the tower $\mathcal{F}$ is *given by the equation* $f(X,Y)=0$ or that $\mathcal{F}$ is *defined recursively by the polynomial* $f(X,Y)$. For a recursive tower $\mathcal{F}=(F_0,F_1,\cdots)$, main information about $\mathcal{F}$ is already contained in the field $F_1=\mathbb{F}_q(x_0,x_1)$.

Definition 2.7. Let $\mathcal{F}$ be a recursive tower over $\mathbb{F}_q$ given by the polynomial $f(X,Y)=0$. Then its *basic function field* is defined as $F=\mathbb{F}_q(x,y)$ where x is a transcendental element over $\mathbb{F}_q$ and y satisfies the relation $f(x,y)=0$.

To explore the ramification and the splitting structure of the whole tower one needs to investigate these structures in both field extensions $F/\mathbb{F}(x)$ and $F/\mathbb{F}(y)$.

Remark 2.8. Many towers in the literature are usually defined by recursive equations of form $g(Y)=h(X)$ where $g(Y)=g_1(Y)/g_2(Y)$ and $h(X)=h_1(X)/h_2(X)$ are rational functions over $\mathbb{F}_q$. Then the polynomial $f(X,Y)$ in Definition 2.6 can be obtained as $f(X,Y)=g_1(Y)h_2(X)-g_2(Y)h_1(X)$.

Let $\mathcal{F}=(F_0,F_1,...)$ be a tower and P be a place of F_j for some $j\geq 0$. If there exists a place Q of F_n for some $n>j$ such that $Q|P$ is *wildly ramified* (i.e., the characteristic of $\mathbb{F}_q$ divides the ramification index $e(Q|P)$), then P is said to be *wildly ramified in the tower* $\mathcal{F}$. Otherwise, the place P is said to be *tame* in $\mathcal{F}$. A tower in which there exists at least one wildly ramified place is called *wild*, otherwise it is called *tame*.

Example 2.9. In [GS96b], Garcia and Stichtenoth defined a tower $\mathcal{G}=(G_0,G_1,...)$ of function fields over $\mathbb{F}_{q^2}$ satisfying $G_0=\mathbb{F}_{q^2}(x_0)$ and $G_{i+1}=G_i(x_{i+1})$ with

$$x_{i+1}^q+x_{i+1}=\frac{x_i^q}{x_i^{q-1}+1} \text{ for } i\geq 0.$$

It is an explicit wild tower recursively defined by equation

$$Y^q+Y=\frac{X^q}{X^{q-1}+1}. \tag{2.4}$$

Let $\Omega:=\{\alpha\in\mathbb{F}_{q^2}\mid \alpha^q+\alpha=0\}$. Here are some interesting properties of the tower $\mathcal{G}$:

(i) The extension G_{i+1}/G_i is Galois of degree $[G_{i+1} : G_i] = q$ for all $i \geq 0$.

(ii) The place $(x_0 = \infty)$ of G_0 is *totally ramified* in the tower $\mathcal{G}$; i.e., there is only one place Q of G_n lying above $(x_0 = \infty)$ with ramification index $e(Q|(x_0 = \infty)) = q^n$.

(iii) The ramification locus is $\mathrm{Ram}(\mathcal{G}/G_0) = \{(x_0 = \beta) \mid \beta \in \Omega \cup \{\infty\}\}$.

(iv) The splitting locus is $\mathrm{Split}(\mathcal{G}/G_0) = \{(x_0 = \alpha) \mid \alpha \in \mathbb{F}_{q^2} \setminus \Omega\}$.

(v) The tower $\mathcal{G}$ is *weakly ramified* (see [Sti09]); i.e., for any places Q of G_n and P of G_0 with $Q|P$, the different exponent is given by $d(Q|P) = 2(e(Q|P) - 1)$.

Therefore the tower is 2-bounded, and by Proposition 2.5 the tower's limit satisfies $\lambda(\mathcal{G}) \geq q - 1$. Then by Drinfeld-Vladut Bound, $\lambda(\mathcal{G}) = q - 1$; i.e., the tower $\mathcal{G}$ is asymptotically optimal.

Let $\mathcal{G} = (G_0, G_1, \cdots)$ and $\mathcal{F} = (F_0, F_1, \cdots)$ be two towers of function fields. We say that $\mathcal{G}$ is a *subtower* of $\mathcal{F}$ if for each integer $i \geq 0$ there exists an integer $j \geq 0$ such that $G_i \subset F_j$.

Proposition 2.10. *[Sti09, Proposition 7.2.8.] If $\mathcal{G}$ is a subtower of $\mathcal{F}$ then $\lambda(\mathcal{G}) \geq \lambda(\mathcal{F})$. In particular, if the tower $\mathcal{F}$ is asymptotically good (resp. optimal), then any subtower $\mathcal{G}$ of $\mathcal{F}$ is also asymptotically good (resp. optimal).*

Some of the towers in the literature are related to each other.

Example 2.11. Let $\mathcal{F} = (F_0, F_1, ...)$ be the tower over $\mathbb{F}_{q^2}$ introduced in [GS95] where $F_0 = \mathbb{F}_{q^2}(x_0)$ and for $i \geq 0$, $F_{i+1} = F_i(z_{i+1})$ where z_{i+1} satisfies

$$z_{i+1}^q + z_{i+1} = x_i^{q+1}, \text{ with } x_i = z_i/x_{i-1} \text{ for } i \geq 1.$$

Then the tower $\mathcal{G}$ in Example 2.9 is actually a subtower of the tower $\mathcal{F}$. In fact, one has

$$z_{i+1}^q + z_{i+1} = x_i^{q+1} = \frac{z_i^{q+1}}{x_{i-1}^{q+1}} = \frac{z_i^{q+1}}{z_i^q + z_i} = \frac{z_i^q}{z_i^{q-1} + 1}. \tag{2.5}$$

It follows that the subfield $\mathbb{F}_{q^2}(z_1, ..., z_{i+1}) \subseteq F_{i+1}$ is isomorphic to the field G_i in the tower $\mathcal{G}$, and hence $\mathcal{G}$ is a subtower of $\mathcal{F}$. That gives another proof for the optimality of the tower in [GS95].

Example 2.12. In [BBGS15] Bassa, Beelen, Garcia and Stichtenoth introduced a new tower $\mathcal{F}/\mathbb{F}_{q^n}$ for any $n \geq 2$ and recursively defined by

$$\mathrm{Tr}_j\left(\frac{Y}{X^{q^{n-j}}}\right) + \mathrm{Tr}_{n-j}\left(\frac{Y^{q^j}}{X}\right) = 1,$$

where $n > j > 0$ with $\gcd(j, n) = 1$ and $\mathrm{Tr}_a(T) := T + T^q + \cdots + T^{q^{a-1}}$ for $a \in \mathbb{N}$. (In the special case $n = 2$ and $j = 1$ one recovers the recursive representation of the optimal tower $\mathcal{F}$ in Example 2.11.) The tower's limit satisfies

$$\lambda(\mathcal{F}/\mathbb{F}_{q^n}) \geq 2\left(\frac{1}{q^j - 1} + \frac{1}{q^{n-j} - 1}\right)^{-1}.$$

For a fixed finite field $\mathbb{F}_{q^n}$ it may give several towers over $\mathbb{F}_{q^n}$ with distinct limits due to the choice of q and the choice of $j < n$. The best lower bound comes from choosing $q = p$ and $j = \lfloor n/2 \rfloor$, see Inequation (2.3).

2.3 Drinfeld modules

It is not clear how one can find such explicit equations in order to construct good towers like in Examples 2.9, 2.11 or 2.12. Moreover, computing the limits for those towers requires very complex and technical calculations. This thesis uses the theory of Drinfeld modular curves to solve such problems.

In this section, we will give a general definition of a Drinfeld module and of a Drinfeld modular curve that will be used in the remainder of the thesis. The definition and the theory of these modules were given by V. Drinfeld in the mid-seventies (see [Dri74, Dri77]). A comprehensive treatment of Drinfeld modules can be found in the treatise of Goss [Gos96]. See also [Gek86] for a more detailed exposition on Drinfeld modular curves. Our aim is to supply the reader with some basic definitions

and facts which are used later in the articles. Many beautiful and deep applications have already been discovered. However, the subject remains young and is under active development.

2.3.1 Preliminaries

Let F be a function field with constant field $\mathbb{F}_q$ and ∞ be a fixed place of degree $\delta \geq 1$. Let $A \subset F$ be the ring of all elements of F whose only poles are at ∞. Prime ideals of A can be identified with places of F distinct from ∞. For an ideal $\mathfrak{n} \subset A$ we define $|\mathfrak{n}| := |A/\mathfrak{n}|$ and $\deg \mathfrak{n} := \log_q |\mathfrak{n}|$. In case $\mathfrak{n} = (a)$ is a principal ideal, we write $\deg a := \deg(a)$. Note that for $a \in A = \mathbb{F}_q[T]$, $\deg a$ is the usual degree of a as a polynomial in T. Let L be an extension field of F together with a homomorphism $\iota : A \to L$. The kernel of ι is called the *A-characteristic* of L. Let $L\{\tau\}$ be a non-commutative polynomial ring generated by the Frobenius endomorphism τ satisfying $\tau a = a^q \tau$ for all $a \in L$. An element $f(\tau) = \sum_{i=0}^{r} a_i \tau^i$ of $L\{\tau\}$ is associated with an additive polynomial $f(X) = \sum_{i=0}^{r} a_i X^{q^i}$. This makes it possible to evaluate elements of $L\{\tau\}$ at elements of $\overline{L}$, the algebraic closure of L. Define $D(f) := a_0$ the constant term of f. If $a_r \neq 0$, we define $\deg f(\tau) = r$.

Definition 2.13. A *Drinfeld A-module* (or a *Drinfeld module* if the ring A is known) *over L of rank $r \in \mathbb{N}^+$* is an injective ring homomorphism

$$\begin{aligned} \phi : A &\to L\{\tau\} \\ a &\mapsto \phi_a, \end{aligned}$$

such that for some $a \in A$, $\phi_a \neq \iota(a)\tau^0$ and for all $a \in A$, $\deg \phi_a = r \deg a$ and $D(\phi_a) = \iota(a)$.

Example 2.14. Let $F = \mathbb{F}_q(T)$ be a rational function field and ∞ be the pole of T. One gets $\delta = \deg \infty = 1$ and $A = \mathbb{F}_q[T]$. In this case we can identify ideals of A with monic polynomials and places of F different from ∞ with monic irreducible polynomials. Since $\mathbb{F}_q[T]$ is generated freely as an algebra over $\mathbb{F}_q$ by T, a Drinfeld $F_q[T]$-module ϕ is determined simply by the element ϕ_T. For instance, let L be some extension field of $\mathbb{F}_q(T)$ and $\iota(T) = 1$. Then a homomorphism $\phi : \mathbb{F}_q[T] \to L\{\tau\}$ specified by

$$\phi_T = -\tau^2 + g\tau + 1$$

is a rank 2 Drinfeld $\mathbb{F}_q[T]$-module of characteristic $\langle T-1\rangle$ over L. The element $\phi_T \in L\{\tau\}$ is associated with the additive polynomial $\phi_T(X) = -X^{q^2}+gX^q+X \in L[X]$. As mentioned before, the element ϕ_T determines ϕ completely. For example the element ϕ_{T^2} can be computed by

$$\begin{aligned}\phi_{T^2} = \phi_T\phi_T &= (-\tau^2+g\tau+1)(-\tau^2+g\tau+1)\\ &= \tau^4+(-g^{q^2}-g)\tau^3+(g^{q+1}-2)\tau^2+2g\tau+1.\end{aligned}$$

Definition 2.15. For an ideal $\mathfrak{n} \subset A$, we define $\phi[\mathfrak{n}]$ to be the set of elements $x \in \overline{L}$ such that $\phi_a(x) = 0$ for all $a \in \mathfrak{n}$. This set is called the set of $\mathfrak{n}$-*torsion points* of ϕ.

If $\mathfrak{n}$ is coprime with the A-characteristic of L then $\phi[\mathfrak{n}]$ is isomorphic to $(A/\mathfrak{n})^r$ as A-modules (see [Ros02, Theorem 13.1.]).

Definition 2.16. Let ϕ and ψ be two Drinfeld A-modules over L. An *isogeny* from ϕ to ψ over L is a non-zero polynomial $\lambda(\tau)$ in $\overline{L}\{\tau\}$ satisfying $\lambda\phi_a = \psi_a\lambda$ for all $a \in A$. If there exists such an isogeny λ between ϕ and ψ, we say that ϕ and ψ are *isogenous*.

Isogenies exist only between Drinfeld modules of the same rank. An isogeny λ is called an *isomorphism* if $\deg\lambda(\tau) = 0$.

Definition 2.17. Let ϕ, ψ be two isogenous Drinfeld modules with isogeny λ. If $\ker\lambda$ is a free $A/\mathfrak{n}$-module of rank one contained in $\phi[\mathfrak{n}]$ for some ideal $\mathfrak{n} \subset A$ then λ is called an $\mathfrak{n}$-*isogeny* and we say that ϕ and ψ are $\mathfrak{n}$-*isogenous*.

Example 2.18. Let us continue Example 2.14. Assume that $\lambda = \tau - u \in \overline{L}\{\tau\}$ is an isogeny between ϕ and another Drinfeld module ψ of the same rank and the same characteristic specified by $\psi_T = h_0\tau^2+h_1\tau+1$. Since $\lambda\phi_a = \psi_a\lambda$ holds for all $a \in \mathbb{F}_q[T]$, the following equalities hold

$$\begin{aligned}\lambda\phi_T &= \psi_T\lambda\\ (\tau-u)(-\tau^2+g\tau+1) &= (h_0\tau^2+h_1\tau+1)(\tau-u)\\ -\tau^3+(g^q+u)\tau^2+(1-ug)\tau-u &= h_0\tau^3+(h_1-h_0u^{q^2})\tau^2+(1-h_1u^q)\tau-u.\end{aligned}$$

Then $h_0 = -1$,

$$g^q+u = h_1+u^{q^2}, \tag{2.6}$$

and

$$ug = h_1 u^q. \tag{2.7}$$

Multiplying both sides of (2.6) by u^q and using (2.7) to cancel the variable h_1, we obtain

$$(ug)^q + u^{q+1} = ug + u^{q^2+q},$$

or

$$(ug - u^{q+1})^q = ug - u^{q+1}.$$

This means that $ug - u^{q+1} = \alpha$ for some $\alpha \in \mathbb{F}_q$. Then

$$g = \frac{\alpha + u^{q+1}}{u} \text{ and } h_1 = \frac{\alpha + u^{q+1}}{u^q} \text{ for } u \neq 0. \tag{2.8}$$

Since $\lambda(\tau) = \tau - u$ is associated with $\lambda(X) = X^q - uX$, the kernel of isogeny λ consists of elements $x \in \overline{L} \setminus \{0\}$ satisfying $x^{q-1} = u$ and $x = 0$. In the case of $\alpha = -1$, from (2.8) one gets $gx^{q-1} - x^{q^2-1} + 1 = 0$ and $\phi_T(x) = -x^{q^2} + gx^q + x = 0$. This means that the element x can be chosen to be a $\langle T \rangle$-torsion point of the Drinfeld module ϕ and λ is a $\langle T \rangle$-isogeny.

2.3.2 Explicit towers from Drinfeld modules

Good towers constructed from Drinfeld modules are based on the property of 'good reduction' of Drinfeld modular curves. In [Gek79] Gekeler investigated (among other things) the Drinfeld modular curve $Y_0(\mathfrak{n})$. In this section, we introduce the notion of Drinfeld modular curve $Y_0(\mathfrak{n})$ in the case of $A = \mathbb{F}_q[T]$. For general rings A see [Gek86]. Since $\mathbb{F}_q[T]$ is a principal ideal domain, the notation $\mathfrak{n}$ can be used for both a monic polynomial and an ideal in $\mathbb{F}_q[T]$.

Definition 2.19. Let $\mathfrak{n} \in A = \mathbb{F}_q[T]$ be a non-zero monic polynomial. The *Drinfeld modular curve* $Y_0(\mathfrak{n})$ contains the points parametrizing isomorphism classes of pairs of $\mathbb{F}_q[T]$-Drinfeld modules of rank 2 together with an $\mathfrak{n}$-isogeny between them.

Example 2.20. Continuing Example 2.18, if we choose $\alpha = -1$ (corresponds to x a T-torsion point of ϕ) then the equations relating g, h_1 and

x simplify to

$$g = \frac{x^{q^2-1}-1}{x^{q-1}} \text{ and } h_1 = \frac{x^{q^2-1}-1}{x^{q^2-q}}.$$

Through this correspondence, we parametrize a pair of rank 2 Drinfeld modules (ϕ, ψ) together with an isogeny of the form $\lambda = \tau - u$ and a non-zero T-torsion point in its kernel. This parametrizing set is not the Drinfeld modular curve $Y_0(T)$ yet. In order to obtain $Y_0(T)$, we need to consider isomorphism classes of Drinfeld modules. Two Drinfeld modules ϕ, ψ with $\phi_T = -\tau^2 + g\tau + 1$ and $\psi_T = -\tau^2 + h_1\tau + 1$ are isomorphic over $\overline{L}$ if there is a non-zero constant $c \in \overline{L}$ such that $c\phi_T = \psi_T c$. From this condition, we see that the constant c must belongs to $\mathbb{F}_{q^2}$ and $g^{q+1} = h_1^{q+1}$ (In this case, the quantity g^{q+1} is called the *j-invariant*[1] of rank 2 Drinfeld module ϕ). Let $Z := x^{q^2-1}$, then g^{q+1} and h_1^{q+1} simplify to

$$g^{q+1} = \left(\frac{x^{q^2-1}-1}{x^{q-1}}\right)^{q+1} = \frac{(Z-1)^{q+1}}{Z}$$

and

$$h_1^{q+1} = \left(\frac{x^{q^2-1}-1}{x^{q^2-q}}\right)^{q+1} = \frac{(Z-1)^{q+1}}{Z^q}.$$

This correspondence now parametrizes the points of $Y_0(T)$.

Adding to $Y_0(\mathfrak{n})$ so-called 'cusps' gives a projective algebraic curve $X_0(\mathfrak{n})$ defined over $\mathbb{F}_q(T)$. In general, however this curve will not be absolutely irreducible. For any prime ideal of A (corresponding to a place of F different from ∞), one obtains by reduction an algebraic curve defined over a finite field. In case of $A = \mathbb{F}_q[T]$ and $\delta = 1$, the curve $X_0(\mathfrak{n})$ (as well as its reduction modulo any prime P relatively prime to $\mathfrak{n}$) is absolutely irreducible. Denoted by $K^{(2)}$ the quadratic extension field of a finite field K. By computing the precise formula for the genus and the number of rational points on reductions of $\mathbb{F}_q[T]$-Drinfeld modular curves $X_0(\mathfrak{n})$, Gekeler showed the following result

Theorem 2.21 ([Gek04])**.** *Let $(\mathfrak{n}_k)_{k\in\mathbb{N}}$ be a series of polynomials of $A = \mathbb{F}_q[T]$ coprime with an irreducible polynomial $P \in A$, and whose degrees*

[1] In general, a rank 2 Drinfeld module ϕ with $\phi_T = \Delta\tau^2 + g\tau + \iota(T)$ has j-invariant $j(\phi) := g^{q+1}/\Delta$.

tend to infinity. Denoted by $\mathbb{F}_P$ the finite field $\mathbb{F}_q[T]/(P)$. Then the family of Drinfeld modular curves $X_0(\mathfrak{n}_k)/\mathbb{F}_P$ attains the Drinfeld–Vladut bound when considered over $\mathbb{F}_P^{(2)}$.

For example in case of $\mathfrak{n}_k = T^k$ and $P = T - 1$, explicit equations for the modular curves $X_0(T^k)$ were given in [Elk01]. Elkies showed in [Elk01] that the reduction of the tower of Drinfeld modular curves $(X_0(T^k))_{k\geq 2}$ at the prime $T - 1$ is a tower satisfying the recursive equation

$$y(y+1)^{q-1} = \frac{x^q}{(x+1)^{q-1}}. \tag{2.9}$$

By Theorem 2.21 this is an optimal tower over $\mathbb{F}_{q^2}$, which was also studied in detail in [BG04]. Moreover, it is a subtower of the tower defined by (2.4). Elkies used this fact to explain the modularity of the optimal tower defined by (2.4).

Example 2.22. One can check that Equation (2.9) satisfies the correspondence in Example 2.20 since they both parametrize $Y_0(T)$. In fact, let $X = x(x+1)^{q-1}$ and $Y = y(y+1)^{q-1}$. Note that $x^q + 1 - (x+1)^{q-1} = x(x+1)^{q-1}$. Then we have

$$\begin{aligned}
\frac{(Y-1)^{q+1}}{Y} &= \frac{\big(y(y+1)^{q-1} - 1\big)^{q+1}}{y(y+1)^{q-1}} = \frac{\left(\frac{x^q}{(x+1)^{q-1}} - 1\right)^{q+1}}{\frac{x^q}{(x+1)^{q+1}}} \\
&= \frac{\big(x^q - (x+1)^{q-1}\big)^{q+1}}{x^q(x+1)^{q^2-q}} = \frac{\big(x(x+1)^{q-1} - 1\big)^{q+1}}{x^q(x+1)^{q^2-q}} \\
&= \frac{(X-1)^{q+1}}{X^q}.
\end{aligned}$$

In [Elk98, Elk01] Elkies found several equations to construct good towers, by studying reductions of Drinfeld-, elliptic- and Shimura-modular curves very explicitly and gave an explanation for the recursive nature of these towers. We will in Chapter 3 give some more general examples (including the defining equations in generic A-characteristic 0).

For $A = \mathbb{F}_q[T]$ and $\delta = 1$ the situation has to a large extent been investigated both theoretically and explicitly. However, we will see in Chapter

4 that generalizations to other rings A and values of δ are possible and that in some cases the resulting families of curves can be described by explicit equations.

Chapter 3

Good towers of function fields

In this chapter, we will give an overview of known and new techniques on how one can obtain explicit equations for candidates of good towers of function fields. The techniques are founded in modular theory (both the classical modular theory and the Drinfeld modular theory). In the classical modular setup, optimal towers can be obtained, while in the Drinfeld modular setup, good towers over any non-prime field may be found. We illustrate the theory with several examples, thus explaining some known towers as well as giving new examples of good explicitly defined towers of function fields. Apart from the shortened introduction, the text of this chapter is as it was published in

[BBN14] A. Bassa, P. Beelen and N. Nguyen, Good towers of function fields, in *Algebraic curves and finite fields*, volume 16 of *Radon Ser. Comput. Appl. Math.*, pages 23–40, De Gruyter, Berlin, 2014.[1]

[1]Alp Bassa is supported by Tübitak Proj. No. 112T233. Peter Beelen and Nhut Nguyen are supported by the Danish National Research Foundation and the National Science Foundation of China (Grant No. 11061130539) for the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography.

3.1 Introduction

In [Elk98, Elk01], Elkies gave a modular interpretation for the tower given in [GS96b] and for all other known optimal recursive towers. More precisely he showed that all known examples of tame, (respectively wild) optimal recursive towers correspond to reductions of classical (respectively Drinfeld) modular curves. Moreover, he found several other equations for such towers, by studying reductions of Drinfeld-, elliptic- and Shimura-modular curves very explicitly and gave an explanation for the recursive nature of these towers. Until now many explicitly known, recursively defined towers have a modular explanation. As an example of this phenomenon, we give a modular interpretation for a good recursive tower given in [LÖ7].

Elkies showed in [Elk01] that the reduction of the tower of Drinfeld modular curves $(X_0(T^n))_{n\geq 2}$ at the prime $T-1$ is a recursive tower satisfying the recursive equation

$$y(y+1)^{q-1} = \frac{x^q}{(x+1)^{q-1}}. \tag{3.1}$$

This is an optimal tower, which was also studied in detail in [BG04]. It is a subtower of the tower in [GS96b]. In this chapter we elaborate further on the ideas of Elkies. Note that the recursive equation in Equation (3.1) has depth one. With this we mean that the variable x_{n+1} in the $(n+1)$-th step of the tower is related to only the previous variables x_n by the recursive equation.

We show how the defining equations for these modular towers can be read off directly from the modular polynomial, and how this, in general, leads to recursions of depth 2. More precisely, we show that the tower can be defined by recursive equations which relate in the $(n+1)$-th step of the tower (for $n \geq 1$), the variable x_{n+1} to both x_n and x_{n-1}. With this approach, finding explicit recursive towers turns out to be an easy task, once the corresponding modular polynomials are known. To illustrate this, we work out the equations for a few cases of Drinfeld modular towers.

In the above Drinfeld modular theory was considered over the polynomial ring $\mathbb{F}_q[T]$. In the last section of the chapter, we study a variation where

this ring is replaced by the coordinate ring of an elliptic curve. We illustrate the ideas by going through a specific example in detail.

3.2 The Drinfeld modular towers $(X_0(P^n))_{n\geq 0}$

In this section we will restrict ourselves to the case of Drinfeld modular curves. However, the classical case of elliptic modular curves is analogous. Therefore we will on occasion state some observation for the classical case also. For more information on Drinfeld modules, the reader is referred to [Gos96, Ros02]. For more information on Drinfeld modular curves, see for example [Gek86]. We denote by $\mathbb{F}$ the field $\mathbb{F}_q(T)$ and let $N \in \mathbb{F}_q[T]$ be a monic polynomial. The field $\mathbb{F}$ will play the role of constant field in the towers we find. From these, towers with a finite field as a constant field can be obtained by reducing the defining equations by a suitably chosen prime element L of $\mathbb{F}_q[T]$. More precisely, the constant field of such a reduced tower is $\mathbb{F}_L := \mathbb{F}_q[T]/(L)$. To describe how to obtain (unreduced) towers, we will use the language of Drinfeld modules.

Let ϕ be a Drinfeld module of rank 2 with j-invariant j_0 and ϕ' be an N-isogenous Drinfeld module with j-invariant j_1. The Drinfeld modular polynomial $\Phi_N(X, Y)$ relates these j-invariants, more precisely it holds that $\Phi_N(j_0, j_1) = 0$. Thinking of j_0 as a transcendental element, we can use this equation to define a so-called Drinfeld modular curve $X_0(N)$. If we want to emphasize the role of N, we will write $j_1 = j_1(N)$. It should be noted that j_0 is independent of N, but it will be convenient to define $j_0(N) := j_0$. The function field $\mathbb{F}(X_0(N))$ of $X_0(N)$ is therefore given by $\mathbb{F}(j_0(N), j_1(N))$. Moreover, it is known, see [Bae92], that

$$[\mathbb{F}(j_0(N), j_1(N)) : \mathbb{F}(j_0(N))] = q^{\deg(N)} \prod_{\substack{P|N \\ P \text{ prime}}} \left(1 + \frac{1}{q^{\deg(P)}}\right). \quad (3.2)$$

In principle the work of finding an explicit description of the function field $\mathbb{F}(X_0(N))$ is done, once the modular polynomial $\Phi_N(X, Y)$ has been computed. However, for general q the Drinfeld modular polynomial is not

known explicitly. Even in the case $N = T$ it has only been determined recently [BB12]. For a given q it can be computed, but this is not always an easy task, since the coefficients of this polynomial tend to get very complicated as the degree of the polynomial N increases. However, following Elkies's ideas ([Elk98, Elk01]) from the modular polynomial $\Phi_P(X, Y)$ for a fixed polynomial P, the function fields of the Drinfeld modular curves $X_0(P^n)$ can be described easily in an explicit way. The reason for this is that for polynomials $P, Q \in \mathbb{F}_q[T]$ a PQ-isogeny can be written as the composite of a P-isogeny and a Q-isogeny, which implies that there is a natural projection from $X_0(PQ)$ to $X_0(P)$ or equivalently an inclusion of function fields $\mathbb{F}(X_0(P)) \subset \mathbb{F}(X_0(PQ))$. This implies that the function field $\mathbb{F}(X_0(P^n))$ also contains the function fields $\mathbb{F}(X_0(P^e))$, for any integer e satisfying $1 \leq e \leq n$, and hence $j_1(P^e) \in \mathbb{F}(X_0(P^n))$. Defining $j_e(P) := j_1(P^e)$ for $e \geq 1$, we see that $j_e(P) \in \mathbb{F}(X_0(P^n))$ for $1 \leq e \leq n$. Since j_0 is independent of P, we also have $j_0(P) = j_0(P^n) \in \mathbb{F}(X_0(P^n))$. Therefore the field $\mathbb{F}(X_0(P^n))$ is the composite of the fields $\mathbb{F}(j_e(P), j_{e+1}(P))$ for $e = 0, \ldots, n-1$. Since $P^{e+1} = PP^e$, any P^{e+1}-isogeny can be written as the composite of a P-isogeny and a P^e-isogeny. This means that $j_e(P)$ and $j_{e+1}(P)$ correspond to P-isogenous Drinfeld modules and hence we have $\Phi_P(j_e(P), j_{e+1}(P)) = 0$ for any e between 0 and $n-1$. We see that $\mathbb{F}(X_0(P^n))$ is the composite of n fields isomorphic to $\mathbb{F}(X_0(P)) = \mathbb{F}(j_0(P), j_1(P))$, the function field of $X_0(P)$. This observation led Elkies to construct a number of recursively defined *towers* $(X_0(P^n))_{n\geq 2}$ of modular curves in [Elk98, Elk01]. In [Elk98] several models defined over $\mathbb{Q}$ of classical modular curves are given, while in [Elk01] the reduction mod $T-1$ of the Drinfeld modular tower $X_0(T^n)_{n\geq 2}$ was described.

We consider the function field of $X_0(P^n)$. We have

$$\mathbb{F}(X_0(P^n)) = \mathbb{F}(j_0(P), j_1(P), \ldots, j_{n-1}(P), j_n(P)).$$

So we can think of $\mathbb{F}(X_0(P^n))$ as iteratively obtained from $\mathbb{F}(j_0(P))$ by adjoining the elements $j_1(P), j_2(P), \ldots, j_n(P)$, where $j_{e+1}(P)$ is a root of the polynomial $\Phi_P(j_e(P), t) \in \mathbb{F}(X_0(P^e))[t]$ for $0 \leq e < n$. However, except for $j_1(P)$ these polynomials are not irreducible. In fact the extension $\mathbb{F}(X_0(P^2))/\mathbb{F}(X_0(P))$ has degree $q^{\deg P}$ by Equation (3.2). This means that the polynomial $\Phi_P(j_1(P), t) \in \mathbb{F}(j_0(P), j_1(P))[t]$ has a factor

$\Psi_P(j_0(P), j_1(P), t)$ of degree $q^{\deg P}$ such that

$$\Psi_P(j_0(P), j_1(P), j_2(P)) = 0.$$

By clearing denominators if necessary, we can assume that

$$\Psi_P(j_0(P), j_1(P), t) \text{ belongs to } \mathbb{F}[j_0(P), j_1(P)][t].$$

Then clearly the trivariate polynomial $\Psi_P(X, Y, Z) \in \mathbb{F}[X, Y, Z]$ satisfies $\Psi_P(j_{e-1}(P), j_e(P), j_{e+1}(P)) = 0$ for all $0 < e < n$. The function field $\mathbb{F}(X_0(P^n))$ can therefore be generated recursively by the equations $\Phi_P(j_0(P), j_1(P)) = 0$ and $\Psi_P(j_{e-1}(P), j_e(P), j_{e+1}(P)) = 0$ for $0 < e < n$. Note that the depth of the recursion is two in general, meaning that to obtain the minimal polynomial of $j_{e+1}(P)$ over $\mathbb{F}(j_0(P), \ldots, j_e(P))$ for $e \geq 1$, we need both $j_e(P)$ and $j_{e-1}(P)$. We arrive at the following proposition.

Proposition 3.1. *Let $P \in \mathbb{F}_q[T]$ be a polynomial and $n \geq 0$ an integer. The function field G_n of the Drinfeld modular curve $X_0(P^n)$ is generated by elements $j_0, \ldots, j_n$ satisfying:*

$$\Phi_P(j_0, j_1) = 0,$$

with $\Phi_P(X, Y)$ the Drinfeld modular polynomial corresponding to P and

$$\Psi_P(j_{e-1}, j_e, j_{e+1}) = 0, \text{ for } 1 \leq e < n,$$

with $\Psi_P(X, Y, Z)$ a suitable trivariate polynomial of Z-degree $q^{\deg P}$. Consequently, the tower of function fields $\mathcal{G} := (G_n)_{n\geq 0}$ can be recursively defined by a recursion of depth two in the following way:

$$G_0 := \mathbb{F}(j_0),$$

$$G_1 := \mathbb{F}(j_0, j_1), \text{ where } \Phi_P(j_0, j_1) = 0$$

and for $n \geq 1$

$$G_{n+1} := G_n(j_{n+1}) \text{ where } \Psi_P(j_{n-1}, j_n, j_{n+1}) = 0.$$

Remark 3.2. The polynomial $\Psi_P(X, Y, Z)$ is easy to describe if P is a prime. In that case $\deg_Y(\Phi_P(X, Y)) = q^{\deg P} + 1$. Since $\Phi_P(X, Y)$ is a symmetric polynomial, it holds that

$$\Phi_P(j_1(P), j_0(P)) = \Phi_P(j_0(P), j_1(P)) = 0.$$

Therefore, the polynomial $\Phi_P(j_1(P), t) \in \mathbb{F}(X_0(P))[t]$ has the factor $t - j_0(P)$. The factor $\Psi(j_0(P), j_1(P), t)$ can be obtained by dividing $\Phi_P(j_1(P), t)$ by $t - j_0(P)$. Note that in this case automatically

$$\deg_t \Psi_P(j_0(P), j_1(P), t) = q^{\deg P} \text{ and } \Psi_P(j_0(P), j_1(P), j_2(P)) = 0,$$

as desired. A similar remark holds for the classical case: if p is a prime number, then the classical modular polynomial $\Phi_p(X, Y)$ is a symmetric polynomial having degree $p + 1$ in both X and Y. The polynomial $\Phi_p(j_1(p), t) \in \mathbb{Q}(j_0(p), j_1(p))[t]$ has a factor of degree one in t (namely $t - j_0(p)$) and a factor of degree p.

By [Sch97] $X_0(P)$ is rational if and only if P has degree one or two. In that case the tower $(\mathbb{F}(X_0(P^n)))_{n\geq 1}$ can be generated in a simpler way. Let $e \geq 1$ and let $u_{e-1}(P)$ be a generating element of $\mathbb{F}(j_{e-1}(P), j_e(P))$ over $\mathbb{F}$. Then $j_{e-1}(P) = \psi(u_{e-1}(P))$ and $j_e(P) = \phi(u_{e-1}(P))$ for certain rational functions $\psi(t) = \psi_0(t)/\psi_1(t)$ and $\phi(t) = \phi_0(t)/\phi_1(t)$. Here $\psi_0(t)$ and $\psi_1(t)$ (resp. $\phi_0(t)$ and $\phi_1(t)$) denote relatively prime polynomials. Since $\mathbb{F}(u_{e-1}(P)) = \mathbb{F}(j_{e-1}(P), j_e(P))$, one can generate the function field of $X_0(P^n)$ for $n \geq 1$ by $u_0(P), \ldots, u_{n-1}(P)$. These generating elements satisfy the equations $\psi(u_e(P)) = \phi(u_{e-1}(P))$ with $1 \leq e < n$, since $\psi(u_e(P)) = j_e(P) = \phi(u_{e-1}(P))$. Similarly as before, one can find generating relations of minimal degree by taking a factor $f_P(u_0(P), t)$ of $\psi_0(t)\phi_1(u_0(P)) - \psi_1(t)\phi_0(u_0(P))$ of degree $q^{\deg P}$ such that $f(u_0(P), u_1(P)) = 0$. The function field $\mathbb{F}(X_0(P^n))$ with $n \geq 1$ can then recursively be defined by the equations $f(u_{e-1}, u_e) = 0$ for $1 \leq e < n$. We arrive at the following proposition.

Proposition 3.3. *Let $P \in \mathbb{F}_q[T]$ be a polynomial of degree one or two and $n \geq 0$ an integer. There exists a bivariate polynomial $f_P(X, Y) \in \mathbb{F}[X, Y]$ of Y-degree $q^{\deg P}$ such that the function field G_n of the Drinfeld modular curve $X_0(P^n)$ is generated by elements $u_0, \ldots, u_{n-1}$ satisfying:*

$$f_P(u_{e-1}, u_e) = 0, \text{ for } 1 \leq e < n.$$

Consequently, the tower of function fields $\mathcal{G} := (G_n)_{n\geq 1}$ can be defined by a recursion of depth one:

$$G_1 := \mathbb{F}(u_0)$$

and for $n \geq 1$

$$G_{n+1} = G_n(u_{n+1}) \text{ where } f_P(u_n, u_{n+1}) = 0.$$

Finally, if P is a polynomial of degree one, then both $X_0(P)$ and $X_0(P^2)$ are rational. In that case, there exist $u_{e-1}(P), u_e(P)$ as above and $v_{e-1}(P)$ such that $\mathbb{F}(u_{e-1}(P), u_e(P)) = \mathbb{F}(v_{e-1}(P))$ for $e > 0$. Similarly as above, there exists rational functions $\psi'(t)$ and $\phi'(t)$ such that $u_{e-1}(P) = \psi'(v_{e-1}(P))$ and $u_e(P) = \phi'(v_{e-1}(P))$. These rational functions have degree $q^{\deg P} = q$, since

$$[\mathbb{F}(v_{e-1}(P)) : \mathbb{F}(u_{e-1}(P))] = [\mathbb{F}(v_{e-1}(P)) : \mathbb{F}(u_e(P))] = q.$$

The function field $\mathbb{F}(X_0(P^n))$ with $n \geq 2$ can then recursively be defined by the equations $\psi'(v_e(P)) = \phi'(v_{e-1}(P))$ for $1 \leq e < n-1$. The depth of the recursion is one (since the defining equation relates $v_e(P)$ to $v_{e-1}(P)$ only) and moreover, the variables can be separated in the defining equations. Since we assume $\deg P = 1$, this puts a heavy restriction on the number of possibilities. In fact, without loss of generality we may assume that $P = T$. In the next section we will describe this case in detail, obtaining explicit equations describing the Drinfeld modular tower $\mathbb{F}(X_0(T^n))_{n\geq 2}$. In the case of classical modular curves, Elkies in [Elk98] gave, among others, several similar examples by considering (prime) numbers p such that the genus of the classical modular curves $X_0(p)$ and $X_0(p^2)$ is zero. This is the case for $p \in \{2, 3, 5\}$.

The towers $(\mathbb{F}(X_0(P^n)))_{n\geq 0}$ are also useful for obtaining interesting towers with finite constant fields, since Gekeler showed the following:

Theorem 3.4 ([Gek04])**.** *Given a prime $L \in \mathbb{F}_q[T]$, denote by $\mathbb{F}_L$ the finite field $\mathbb{F}_q[T]/(L)$. Moreover, write $\mathbb{F}_L^{(2)}$ for the quadratic extension of $\mathbb{F}_L$. The reduction modulo any prime $L \in \mathbb{F}_q[T]$ not dividing P of the tower $(X_0(P^n))_{n\geq 0}$ gives rise to an asymptotically optimal tower over the constant field $\mathbb{F}_L^{(2)}$.*

The above theorem implies that the tower found in [Elk01], being the reduction of $(X_0(T^n))_{n\geq 0}$ modulo $T-1$, is asymptotically optimal over the constant field $\mathbb{F}_{T-1}^{(2)} = \mathbb{F}_{q^2}$. Now we will give several examples. Sometimes we do not give all details, since this would fill many pages. Several computations were carried out using the computer algebra package Magma [BCP97]. For example all Drinfeld modular polynomials below were calculated using Magma. On occasion, we will perform all calculations sketched above for a reduced version of the tower $(\mathbb{F}(X_0(P^n)))_{n\geq 0}$,

since the resulting formulas are usually much more compact after reduction. In all examples in this section, it is assumed that $q = 2$, while P will be a polynomial of degree one or two.

Example 3.5 ($P = T, q = 2$)**.** By [Sch95], the Drinfeld modular polynomial of level T in case $q = 2$ is given by

$$\Phi_T(X,Y) = X^3 + Y^3 + T(T+1)^3(X^2+Y^2) + T^2(T+1)^6(X+Y) \\ + T^3(T+1)^9 + X^2Y^2 + (T+1)^3(T^2+T+1)XY + T(X^2Y + XY^2).$$

The polynomial $\Psi_T(X,Y,Z)$ can readily be found using Remark 3.2:

$$\Psi_T(X,Y,Z) = Z^2 + (X + (Y^2 + TY + T(T+1)^3))Z + X^2 \\ + (Y^2 + TY + T(T+1)^3)X + TY^2 \\ + (T^2+T+1)(T+1)^3Y + T^2(T+1)^6.$$

Using Proposition 3.1, we can in principle now describe the tower of function fields of the modular curves $(X_0(T^n))_{n\geq 0}$. However, we can use Proposition 3.3 to find a recursive description of depth one. First we need a uniformizing element u_0 of $\mathbb{F}(j_0, j_1)$. Using a computer, one finds

$$u_0 = \frac{T^3(T^2j_0 + T^2 + T^4 + T^6 + 1 + Tj_1 + T^2j_1 + Tj_0 + j_0j_1)}{(T^3 + j_1^2 + T^2 + j_0 + Tj_1 + T^3j_0 + T^7 + T^4j_1 + T^6}.$$

Expressing j_0 and j_1 turns out to give a more compact formula.

$$j_0 = \frac{(u_0+T)^3}{u_0} \text{ and } j_1 = \frac{(u_0+T^2)^3}{u_0^2}.$$

This means that the variables u_0 and u_1 satisfy the equation:

$$\frac{(u_0+T^2)^3}{u_0^2} = \frac{(u_1+T)^3}{u_1}.$$

However, this is not an equation of minimal degree. As explained before Proposition 3.3, we can find an equation of degree (in this case) two by factoring:

$$(X+T^2)^3Y + (Y+T)^3X^2 = (XY+T^3)(X^2 + XY^2 + XYT + YT^3).$$

We find that $f_T(X,Y) = X^2 + XY^2 + XYT + YT^3$. This polynomial recursively defines the tower of function fields of the modular curves $(X_0(T^n))_{n\geq 1}$ as in Proposition 3.3.

Example 3.6 ($P = T^2+T+1, q = 2$)**.** The Drinfeld modular polynomial of level $T^2 + T + 1$ is given by

$$\begin{aligned}\Phi_{T^2+T+1}(X,Y) = {} & X^5 + Y^5 + X^4Y^4 + (T^2+T+1)(X^4Y^2 + X^2Y^4) \\ & + (T^2+T+1)(X^4Y + XY^4) \\ & + T^3(T+1)^3(T^2+T+1)(X^4 + Y^4) \\ & + T^2(T+1)^2(T^2+T+1)X^3Y^3 \\ & + (T^2+T)(T^2+T+1)(T^3+T+1)(T^3+T^2+1)(X^3Y^2 + X^2Y^3) \\ & + T^3(T+1)^3(T^2+T+1)(X^3Y + XY^3) \\ & + T^6(T+1)^6(T^2+T+1)^2(X^3 + Y^3) \\ & + T^5(T+1)^5(T^2+T+1)(T^4+T+1)X^2Y^2 \\ & + T^6(T+1)^6(T^2+T+1)(T^4+T+1)(X^2Y + XY^2) \\ & + T^9(T+1)^9(T^2+T+1)^3(X^2 + Y^2) + T^{11}(T+1)^{11}XY.\end{aligned}$$

As in the previous example one can use Remark 3.2, to find the trivariate polynomial $\Psi_{T^2+T+1}(X,Y,Z)$. Finding a uniformizing element u_0 of $\mathbb{F}(X_0(T^2+T+1))$ is somewhat more elaborate. Since such a uniformizing element fills several pages, it is omitted. Below we will state the reduction of u_0 modulo T and $T+1$, so the reader can get an impression of its form. Once u_0 is found, j_0 and j_1 can be expressed in terms of it. In this case we find:

$$j_0 = \frac{(u_0+1)^3(u_0^2+u_0+T^2+T+1)}{u_0}$$

and

$$j_1 = \frac{(u_0+T^2+T+1)^3(u_0^2+u_0+T^2+T+1)}{u_0^4}.$$

To find the polynomial $f_{T^2+T+1}(X,Y)$, we need to factor the polynomial

$$(Y^5 + (T^2+T+1)Y^3 + (T^2+T+1)Y^2 + (T^2+T)Y + (T^2+T+1))X^4 + Y(X^5 + (T^2+T)X^4 + (T^2+T+1)^2X^3 + (T^2+T+1)^3X^2 + (T^2+T+1)^4),$$

whose factors are $XY + T^2 + T + 1$ and

$$\begin{aligned}f_{T^2+T+1}(X,Y) = {} & Y^4X^3 + (T^2+T+1)(Y^3X^2 + Y^2X^3 + (T^2+T+1)Y^2X \\ & + YX^3 + (T^2+T+1)YX^2 + (T^2+T+1)^2Y) + X^4.\end{aligned}$$

The polynomial $f_{T^2+T+1}(X,Y)$ recursively defines the tower of function fields of the modular curves $(X_0((T^2+T+1)^n))_{n\geq 1}$ as in Proposition 3.3.

We consider the reduction modulo T or $T+1$ of this tower, which by Theorem 3.4 gives an optimal tower over $\mathbb{F}_4$. While a uniformizing element of $\mathbb{F}(X_0(T^2+T+1))$ was too long to be stated, over $\mathbb{F}_4(X_0(T^2+T+1))$ it is given by

$$u_0 := \frac{j_0^4 j_1^3 + j_0^4 j_1^2 + j_0^4 j_1 + j_0^4 + j_0^3 j_1^7 + j_0^3 j_1^6 + j_0^3 j_1^4 + j_0^2 j_1^5 + j_0 j_1^5 + j_0 j_1^4 + j_1^6 + j_1^4}{j_1^8}.$$

Reducing the above found polynomial $f_{T^2+T+1}(X,Y)$ modulo T or $T+1$, we now explicitly find that the polynomial

$$Y^4X^3 + Y^3X^2 + Y^2X^3 + Y^2X + YX^3 + YX^2 + Y + X^4$$

recursively defines an optimal tower over $\mathbb{F}_4$.

Example 3.7 $(P = T^2 + T, q = 2)$**.** In the previous examples, the polynomial P was a prime, but in this example we will consider the composite polynomial $P = T^2+T$. The Drinfeld modular polynomial of level T^2+T

has Y-degree 9 by Equation 3.2. Using a computer, one finds:

$$\begin{aligned}
&\Phi_{T^2+T}(X,Y) = X^9+Y^9+(X^8Y^4+X^4Y^8)+(T^2+T+1)(X^8Y^2+X^2Y^8)\\
&+(T^2+T)(X^8Y+XY^8)+(T^6+T^5+T^3+T^2+1)(T^2+T)(X^8+Y^8)\\
&+(X^7Y^4+X^4Y^7)+(T^2+T)^3(X^7Y^3+X^3Y^7)\\
&+(T^5+T^4+T^3+T+1)(T^5+T^3+T^2+T+1)(T^2+T)^3(X^7+Y^7)\\
&+(X^6Y^5+X^5Y^6)+(X^6Y^4+X^4Y^6)+(T^2+T+1)^5(X^6Y^3+X^3Y^6)\\
&+(T^7+T^6+T^5+T^4+T^2+T+1)(T^7+T^3+T^2+T+1)(T^2+T)(X^6Y^2+X^2Y^6)\\
&+(T^{14}+T^{13}+T^{11}+T^{10}+T^7+T^5+T^4+T^2+1)(T^2+T)^2(X^6Y+XY^6)\\
&+(T^4+T+1)(T^2+T+1)(T^2+T)^5(T^8+T^6+T^5+T^4+T^3+T+1)(X^6+Y^6)\\
&+X^5Y^5+(T^2+T+1)(T^2+T)^2(X^5Y^4+X^4Y^5)+(T^2+T)^2(X^5Y^3+X^3Y^5)\\
&+(T^9+T^8+T^7+T^5+1)(T^9+T^7+T^6+T^3+T^2+T+1)(X^5Y^2+X^2Y^5)\\
&+(T^6+T^5+T^2+T+1)(T^6+T^5+1)(T^2+T+1)^3(T^2+T)^2(X^5Y+XY^5)\\
&+(T^5+T^3+T^2+T+1)(T^5+T^4+T^3+T+1)(T^2+T+1)(T^2+T)^5(X^5+Y^5)\\
&+(T^{18}+T^{17}+T^{16}+T^{10}+T^9+T^4+T^2+T+1)(T^2+T+1)^2(T^2+T)(X^4Y^2+X^2Y^4)\\
&+(T^2+T+1)^2(T^2+T)^7(X^4Y+XY^4)+(T^2+T)^8(T^6+T^5+T^3+T^2+1)(X^4+Y^4)\\
&+(T^{10}+T^9+T^8+T^6+T^5+T+1)(T^2+T+1)^3X^3Y^3+(T^8+T^7+T^2+T+1)\\
&\cdot(T^8+T^7+T^6+T^5+T^4+T^3+1)(T^2+T+1)(T^2+T)^2(X^3Y^2+X^2Y^3)\\
&+(T^2+T+1)(T^2+T)^4(T^{10}+T^9+T^8+T^3+T^2+T+1)(X^3Y+XY^3)\\
&+(T^4+T+1)(T^3+T+1)(T^3+T^2+1)(T^2+T+1)^3(T^2+T)^3X^2Y^2\\
&+(T^2+T)^{10}(X^2Y+XY^2)+(T^2+T)^{10}(X^2+Y^2)+(T^4+T+1)(T^2+T)^7(X^3+Y^3)\\
&+(T^3+T+1)(T^3+T^2+1)(T^2+T)^6XY+(T^2+T+1)(T^2+T)^8(X+Y)+(T^2+T)^9.
\end{aligned}$$

Finding a uniformizing element u_0 of $\mathbb{F}(X_0(T^2+T))$ and expressing j_0 and j_1 in it, we find

$$j_0 = \frac{(u_0^3+(T^2+T)u_0+(T^2+T))^3}{u_0(u_0+T)^2(u_0+T+1)^2} \text{ and } j_1 = \frac{(u_0^3+(T^2+T)u_0^2+(T^2+T)^2)^3}{u_0^4(u_0+T)^2(u_0+T+1)^2}.$$

To find $f_{T^2+T}(X,Y)$, we need to factor a bivariate polynomial of Y-degree 9. Note that Remark 3.2 does not apply, though it still predicts the existence of one factor of Y-degree one. The factors turn out to be

$$XY+T^2+T,$$

$$Y^2X^2+TY^2X+(T^2+T)YX+(T^3+T^2)Y+T^2X^2+T^4+T^2,$$

$$Y^2X^2+(T+1)Y^2X+(T^2+T)YX+(T^3+T)Y+(T^2+1)X^2+T^4+T^2,$$

and

$$\begin{aligned} &Y^4X^3+Y^4X^2+(T^2+T)Y^4X+(T^2+T)Y^3X^2+(T^2+T)Y^3X\\ &+(T^4+T^2)Y^3+(T^2+T+1)Y^2X^3+(T^4+T^2)Y^2X+(T^4+T^2)Y^2\\ &+(T^2+T)YX^3+(T^4+T)YX^2+(T^6+T^5+T^4+T^3)Y+X^4. \end{aligned}$$

The last factor is $f_{T^2+T}(X,Y)$, since it is the only factor of Y-degree 4. Considering reduction modulo T^2+T+1, we see by Theorem 3.4 that the polynomial

$$Y^4X^3+Y^4X^2+Y^4X+Y^3X^2+Y^3X+Y^3+Y^2X+Y^2+YX^3+Y+X^4$$

recursively defines an optimal tower over $\mathbb{F}_{16}$.

3.3 An example of a classical modular tower

In [LÖ7, Section 6.1.2.3] a good recursive tower over the field $\mathbb{F}_{7^4}$ is given. The recursive equation stated there is:

$$y^5=\frac{x^5+5x^4+x^3+2x^2+4x}{2x^4+5x^3+2x^2+x+1}.$$

We will consider the equivalent tower obtained by replacing x by $3x$ and y by $3y$. The resulting equation is:

$$y^5=x\frac{x^4-3x^3+4x^2-2x+1}{x^4+2x^3+4x^2+3x+1}. \tag{3.3}$$

The proof that the corresponding recursive tower is good can be carried out by observing that there are places that split completely in the tower and by observing that the ramification locus of the tower is finite. Since all ramification is tame (the steps in the tower are Kummer extensions), the Riemann-Hurwitz genus formula can be used directly to estimate the genera of the function fields occurring in the tower. In this way one obtains that the limit of the tower is at least 6. The splitting places of this tower are not defined over $\mathbb{F}_{49}$, otherwise this would be an optimal tower. We will show in this section that this tower has a modular interpretation and obtain a generalization to other characteristics as well.

Based on the extension degrees, a reasonable supposition is that there may be a relation to the function fields of the curves $X_0(5^n)_{n\geq 1}$. In [Elk98] Elkies found an explicit recursive description of $X_0(5^n)_{n\geq 2}$: define $P(t) := t^5 + 5t^3 + 5t - 11$, then this tower satisfies the recursive equation

$$P(y) = \frac{125}{P\left(\frac{x+4}{x-1}\right)},$$

or equivalently

$$y^5 + 5y^3 + 5y - 11 = \frac{(x-1)^5}{x^4 + x^3 + 6x^2 + 6x + 11}. \tag{3.4}$$

The steps in this tower are not Galois, but Elkies notes that the polynomial $P(X)$ is dihedral. More concretely: $P(v^{-1} - v) = -v^5 - 11 + v^{-5}$. Since the steps in the recursive tower from equation (3.3) are Galois (note that the 5-th roots of unity belong to the constant field), we consider the extension $\mathbb{Q}(v)$ of $\mathbb{Q}(x)$ defined by $1/v - v = x$. Direct verification using Magma reveals that the function field $\mathbb{Q}(v, y)$ contains a solution w to the equation $1/w - w = y$ such that

$$w^5 = v(v^4 - 3v^3 + 4v^2 - 2v + 1)/(v^4 + 2v^3 + 4v^2 + 3v + 1).$$

Therefore we recover equation (3.3). We have shown that the tower satisfying equation (3.3) recursively, is a supertower of the modular tower $X_0(5^n)_{n\geq 2}$. One can say more however. Equation (3.3) occurs in the literature of modular functions. In fact it occurs in the same form in the famous first letter that S. Ramanujan wrote 100 years ago to G.H. Hardy. In it, Ramanujan defined a continued fraction, now known as the Rogers–Ramanujan continued fraction, and related two of its values by equation (3.3) (see Theorem 5.5 in [BCH$^+$99] for more details). The Rogers–Ramanujan continued fraction can be seen as a modular function for the full modular group $\Gamma(5)$ and defines a uniformizing element of the function field $\mathbb{Q}(X(5))$. This means that we can obtain the recursive tower defined (over $\mathbb{Q}$) by equation (3.3) as a lift of the tower defined by equation (3.4) by extending the first function field of that tower to the function field of $X(5)$. Also by direct computation one sees that the extension $\mathbb{Q}(\zeta_5)(w, x)/\mathbb{Q}(\zeta_5)(x)$ is a Galois extension (it is in fact the Galois closure of $\mathbb{Q}(\zeta_5)(x, y)/\mathbb{Q}(\zeta_5)(x)$).

For any prime number p different from 5 the curves have good reduction, meaning that we may reduce the equations modulo such primes p.

Extending the constant field to $\mathbb{F}_q$ with $q = p^2$ if $p \equiv \pm 1 \pmod 5$ and $q = p^4$ if $p \equiv \pm 2 \pmod 5$, we make sure that the primitive fifth root of unity is contained in the constant field $\mathbb{F}_q$. Over this constant field, the tower satisfying the recursive relation (3.3) has limit at least $p - 1$; i.e., the ratio of the number of rational places and the genus tends to a value larger than or equal to $p-1$ as one goes up in the tower. This means that the tower is optimal if $p \equiv \pm 1 \pmod 5$ and good if $p \equiv \pm 2 \pmod 5$.

3.4 A tower obtained from Drinfeld modules over a different ring

Previously we have used Drinfeld modules of rank 2 over the ring $\mathbb{F}_q[T]$ to construct towers of function fields. In principle, one can consider Drinfeld modules over other rings and use them to construct towers of function fields. The theory is however, much less explicit in this case. In this section, we illustrate the method of constructing towers by studying a particular example in detail. More precisely, we consider Drinfeld modules over the ring $A := \mathbb{F}_2[S,T]/\langle S^2 + S - T^3 - T\rangle$. The ring A is the coordinate ring of an elliptic curve with 5 rational points. We denote by P the prime ideal of A generated by (the classes of) S and T. This prime ideal corresponds to the point $(0,0)$ of the elliptic curve. We will construct an asymptotically good tower in this setup.

3.4.1 Explicit Drinfeld modules of rank 2

Unlike in the case of Drinfeld modules over the ring $\mathbb{F}_q[T]$ we cannot directly compute a modular polynomial. In fact, it is non-trivial even to compute examples of Drinfeld modules ϕ of rank 2 in this setting. Our first task will be to compute all possible normalized Drinfeld modules of rank 2 over A in characteristic P. Such a Drinfeld module ϕ is specified by

$$\phi_T = \tau^4 + g_1\tau^3 + g_2\tau^2 + g_3\tau \tag{3.5}$$

and

$$\phi_S = \tau^6 + h_1\tau^5 + h_2\tau^4 + h_3\tau^3 + h_4\tau^2 + h_5\tau. \tag{3.6}$$

The eight parameters $g_1, \ldots, h_5$ cannot be chosen independently, but should be chosen such that $\phi_{S^2+S-T^3-T} = \phi_0 = 0$ and $\phi_T\phi_S = \phi_S\phi_T$. The first condition comes from the defining equation of the curve, while the second one should hold, since the fact the ϕ is a homomorphism implies that $\phi_T\phi_S = \phi_{TS}$ and $\phi_S\phi_T = \phi_{ST} = \phi_{TS}$. In this way one obtains the following system of polynomial equations for g_i and h_j. From the condition $\phi_{S^2+S-T^3-T} = 0$ one obtains that the g_i and h_j are in the zero-set of the following polynomials:

$$
\begin{aligned}
&h_5 + g_3,\\
&h_4 + h_5^3 + g_2,\\
&h_3 + h_4^2h_5 + h_4h_5^4 + g_1 + g_3^7,\\
&h_2 + h_3^2h_5 + h_3h_5^8 + h_5^5 + g_2^4g_3^3 + g_2^2g_3^9 + g_2g_3^{12} + 1,\\
&h_1 + h_2^2h_5 + h_2h_5^{16} + h_3^4h_4 + h_3h_4^8 + g_1^4g_3^3 + g_1^2g_3^{17} + g_1g_3^{24} + g_2^{10}g_3 + g_2^9g_3^4 + g_2^5g_3^{16},\\
&h_1^2h_5 + h_1h_5^{32} + h_2^4h_4 + h_2h_4^{16} + h_3^9 + g_1^8g_2^2g_3 + g_1^8g_2g_3^4 + g_1^4g_2g_3^{32} + g_1^2g_2^{16}g_3 + g_1g_2^{16}g_3^8\\
&+g_1g_2^8g_3^{32} + g_2^{21} + g_3^{48} + g_3^{33} + g_3^3 + 1,\\
&h_1^4h_4 + h_1h_4^{32} + h_2^8h_3 + h_2h_3^{16} + h_5^{64} + h_5 + g_1^{18}g_3 + g_1^{17}g_3^8 + g_1^{16}g_2^5 + g_1^9g_3^{64} + g_1^4g_2^{33}\\
&+g_1g_2^{40} + g_2^{32}g_3^{16} + g_2^{32}g_3 + g_2^{16}g_3^{64} + g_2^2g_3 + g_2g_3^{64} + g_2g_3^4,\\
&h_1^8h_3 + h_1h_3^{32} + h_2^{17} + h_4^{64} + h_4 + g_1^{36}g_2 + g_1^{33}g_2^8 + g_1^{32}g_3^{16} + g_1^{32}g_3 + g_1^{16}g_3^{128} + g_1^9g_2^{64}\\
&+g_1^2g_3 + g_1g_3^{128} + g_1g_3^8 + g_2^{80} + g_2^{65} + g_2^5,\\
&h_1^{16}h_2 + h_1h_2^{32} + h_3^{64} + h_3 + g_1^{73} + g_1^{64}g_2^{16} + g_1^{64}g_2 + g_1^{16}g_2^{128} + g_1^4g_2 + g_1g_2^{128} + g_1g_2^8\\
&+g_3^{256} + g_3^{16} + g_3,\\
&h_1^{33} + h_2^{64} + h_2 + g_1^{144} + g_1^{129} + g_1^9 + g_2^{256} + g_2^{16} + g_2,\\
&h_1^{64} + h_1 + g_1^{256} + g_1^{16} + g_1.
\end{aligned}
$$

Similarly, the condition $\phi_T\phi_S = \phi_S\phi_T$ gives rise to the following polynomials:

$$
\begin{aligned}
&h_5^2g_3 + h_5g_3^2,\\
&h_4^2g_3 + h_4g_3^4 + h_5^4g_2 + h_5g_2^2,\\
&h_3^2g_3 + h_3g_3^8 + h_4^4g_2 + h_4g_2^4 + h_5^8g_1 + h_5g_1^2,\\
&h_2^2g_3 + h_2g_3^{16} + h_3^4g_2 + h_3g_2^8 + h_4^8g_1 + h_4g_1^4 + h_5^{16} + h_5,\\
&h_1^2g_3 + h_1g_3^{32} + h_2^4g_2 + h_2g_2^{16} + h_3^8g_1 + h_3g_1^8 + h_4^{16} + h_4,\\
&h_1^4g_2 + h_1g_2^{32} + h_2^8g_1 + h_2g_1^{16} + h_3^{16} + h_3 + g_3^{64} + g_3,\\
&h_1^8g_1 + h_1g_1^{32} + h_2^{16} + h_2 + g_2^{64} + g_2,\\
&h_1^{16} + h_1 + g_1^{64} + g_1.
\end{aligned}
$$

One could attempt a direct Groebner basis computation on the ideal $I \subset \mathbb{F}_2[g_1, \ldots, h_5]$ generated by the above two sets of polynomials, but we can simplify the system of polynomial equations first. Taking for example the last of each set of polynomials, $p_1 := h_1^{64} + h_1 + g_1^{256} + g_1^{16} + g_1$ and $p_2 := h_1^{16} + h_1 + g_1^{64} + g_1$, we find that $p_3 := p_1 - p_2^4 = h_1^4 + h_1 + g_1^{16} + g_1^4 + g_1$ is an element of the ideal I. Moreover, since $p_2 = p_3 + p_3^4$ and $p_1 = p_3 + p_3^4 + p_3^{16}$, we can replace p_1 and p_2 by p_3 when generating the ideal

I. Also we can eliminate the variables h_i altogether, since they can be expressed in terms of g_1, g_2, g_3 using the first five generators of I. After performing these and similar simplifications, we computed a Groebner basis of the resulting polynomial ideal in the variables g_1, g_2 and g_3 using Magma. The resulting Groebner basis contains one irreducible (but not absolutely irreducible) polynomial involving only g_2 and g_3 as well as an irreducible polynomial of degree one in g_1. This means that the zero-set of the ideal I can be interpreted as an irreducible algebraic curve defined over $\mathbb{F}_2$. It turns out to have genus 4.

From the modular point of view, it is more natural to consider isomorphism classes of Drinfeld modules. An isomorphism between two Drinfeld modules ϕ and ψ is given by a non-zero constant c such that $c\phi = \psi c$. Considering equations (3.5) and (3.6), we see that for normalized Drinfeld modules ϕ and ψ we have that $c \in \mathbb{F}_4$ and that $g_1^3, g_2, g_3^3, h_1^3, h_2, h_3^3, h_4, h_5^3$ are invariant under isomorphism. Inspecting the Groebner basis computation performed before, we obtain a polynomial relation between $g := g_3^3$ and g_2 and a way to express all other invariants in these two parameters. These polynomials are too large to state here, so we will not do so. The important fact is that we again obtain an irreducible algebraic curve defined over $\mathbb{F}_2$ which determines the isomorphism classes of possible rank 2 Drinfeld modules. This modular curve is known to have genus zero and to be irreducible, but not absolutely irreducible, see [Gek86]. There it is also shown that the number of components is equal to the class number h_E, over which extension field these components are defined and how the Galois group of this extension acts on the components. In our case we obtain that there are 5 components defined over $\mathbb{F}_{32}$ and that the Frobenius map of $\mathbb{F}_{32}/\mathbb{F}_2$ acts transitively on these five components. One such component is determined by the following relation between g and g_2:

$$
\begin{aligned}
&g_2^{13} + (\alpha^5 g + \alpha^{14}) g_2^{12} + (\alpha^4 g^2 + \alpha^{19} g + \alpha^7) g_2^{11} + (\alpha^9 g^3 + \alpha^{18} g^2 + \alpha^9 g + \alpha^{21}) g_2^{10} \\
&+(\alpha^{10} g^4 + \alpha^{21} g^3 + \alpha^{16} g^2 + \alpha^{18} g + \alpha^8) g_2^9 + (\alpha^{15} g^5 + \alpha^{29} g^4 + \alpha^{10} g^3 + \alpha^{27} g^2 + \alpha^{25} g + \alpha^8) g_2^8 \\
&+(g^6 + \alpha^{28} g^5 + \alpha^6 g^4 + \alpha^{11} g^3 + \alpha^6 g^2 + \alpha^{28} g + \alpha^9) g_2^7 \\
&+(\alpha^5 g^7 + \alpha^{23} g^6 + \alpha^2 g^5 + \alpha^{15} g^4 + \alpha^{12} g^3 + \alpha^4 g^2 + \alpha^6 g + \alpha^{25}) g_2^6 \\
&+(\alpha^4 g^8 + \alpha^{30} g^7 + \alpha^{18} g^6 + \alpha^3 g^5 + \alpha^{15} g^4 + \alpha^{12} g^3 + \alpha^{23} g^2 + \alpha^{29} g + \alpha^{10}) g_2^5 \\
&+(\alpha^9 g^9 + \alpha^{25} g^8 + \alpha^8 g^7 + \alpha g^6 + \alpha^7 g^5 + \alpha^{25} g^4 + \alpha^{23} g^3 + \alpha^{15} g^2 + \alpha g + \alpha^{26}) g_2^4 \\
&+(\alpha^4 g^{10} + \alpha^{27} g^9 + \alpha^{15} g^8 + \alpha^{11} g^7 + \alpha^5 g^6 + \alpha^{26} g^5 + \alpha^{18} g^4 + \alpha^9 g^3 + \alpha^{11} g^2 + \alpha^{30} g) g_2^3 \\
&+(\alpha^9 g^{11} + \alpha^{30} g^{10} + \alpha^{10} g^9 + \alpha^{15} g^8 + \alpha^{12} g^7 + \alpha^6 g^6 + \alpha^2 g^5 + \alpha^{26} g^4 + \alpha^{15} g^3 + \alpha^6 g^2 \\
&+\alpha^{13} g + \alpha^{30}) g_2^2 + (\alpha^{10} g^{12} + \alpha^{16} g^{11} + \alpha^4 g^{10} + \alpha^{12} g^9 + \alpha^{18} g^8 + \alpha^{28} g^7 + \alpha^2 g^6 + \alpha^9 g^5 \\
&+\alpha^3 g^4 + \alpha^8 g^3 + \alpha^{10} g^2 + \alpha^{17} g) g_2 + \alpha^{15} g^{13} + \alpha^5 g^{12} + \alpha^{24} g^{11} + \alpha^4 g^{10} + \alpha^{11} g^9 + \alpha^8 g^8 \\
&+\alpha^{12} g^7 + \alpha^{27} g^6 + g^5 + \alpha^{23} g^4 + \alpha^{19} g^3 + \alpha^8 g^2 + \alpha^{24} g + 1,
\end{aligned}
$$

with $\alpha^5 + \alpha^2 + 1 = 0$.

Using this polynomial, we can define a rational function field $\mathbb{F}_{32}(g_2, g)$. Since it is rational, there exists a uniformizer $u \in \mathbb{F}_{32}(g_2, g)$ such that $\mathbb{F}_{32}(g_2, g) = \mathbb{F}_{32}(u)$. Finding such element u can easily be done using Magma. Note that this element u plays a very similar role as the element j_0 in Section 3.2, since it describes isomorphism classes of rank 2 Drinfeld modules. The only difference is that now there exist five conjugated families of isomorphism classes, whereas previously there was only one such family.

3.4.2 Finding an isogeny

To find a tower, we need to find an isogeny from a given Drinfeld module to another. That is to say: we need to find two Drinfeld modules ϕ and ψ both of rank 2 and an additive polynomial λ such that $\lambda\phi = \psi\lambda$. We will describe the most direct approach, not using the theory of torsion points, which would give a faster way to obtain isogenies. We will find an isogeny λ of the simplest possible form $\lambda = \tau - a$ from ϕ to another Drinfeld module ψ specified by

$$\psi_T := \tau^4 + l_1\tau^3 + l_2\tau^2 + l_3\tau$$

and

$$\psi_S = \tau^6 + t_1\tau^5 + t_2\tau^4 + t_3\tau^3 + t_4\tau^2 + t_5\tau.$$

Since we can describe both ϕ and ψ essentially using only one parameter, we can obtain a relation between these parameters and a. More in detail, always assuming $q = 2$, we have

$$\lambda\phi_T = \psi_T\lambda \tag{3.7}$$

and

$$\lambda\phi_S = \psi_S\lambda. \tag{3.8}$$

The left hand side of equation (3.7) is

$$\begin{aligned}&(\tau - a)(\tau^4 + g_1\tau^3 + g_2\tau^2 + g_3\tau)\\ &= \tau^5 + (g_1^q - a)\tau^4 + (g_2^q - ag_1)\tau^3 + (g_3^q - ag_2)\tau^2 - ag_3\tau,\end{aligned}$$

while the right hand one is

$$\begin{aligned}&(\tau^4 + l_1\tau^3 + l_2\tau^2 + l_3\tau)(\tau - a)\\ &= \tau^5 + (l_1 - a^{q^4})\tau^4 + (l_2 - l_1 a^{q^3})\tau^3 + (l_3 - l_2 a^{q^2})\tau^2 - l_3 a^q \tau.\end{aligned}$$

Consequently we get

$$\begin{cases} g_1^q - a & = l_1 - a^{q^4} \\ g_2^q - ag_1 & = l_2 - l_1 a^{q^3} \\ g_3^q - ag_2 & = l_3 - l_2 a^{q^2} \\ -ag_3 & = -l_3 a^q. \end{cases}$$

By substitution top down, we can eliminate variables l_1, l_2, l_3 and get

$$(g_1 a^{q^2+q+1} + g_2 a^{q+1} + g_3 a + a^{q^3+q^2+q+1})^q - (g_1 a^{q^2+q+1} + g_2 a^{q+1} + g_3 a + a^{q^3+q^2+q+1}) = 0$$

or

$$a^{q^3+q^2+q+1} + g_1 a^{q^2+q+1} + g_2 a^{q+1} + g_3 a = \gamma \in \mathbb{F}_q. \tag{3.9}$$

Equation (3.9) can be seen as a polynomial in terms of a, u and g_3.

Similarly, studying equation (3.8), we obtain

$$\begin{cases} h_1^q - a & = t_1 - a^{q^6} \\ h_2^q - ah_1 & = t_2 - t_1 a^{q^5} \\ h_3^q - ah_2 & = t_3 - t_2 a^{q^4} \\ h_4^q - ah_3 & = t_4 - t_3 a^{q^3} \\ h_5^q - ah_4 & = t_5 - t_4 a^{q^2} \\ -ah_5 & = -t_5 a^q. \end{cases}$$

Also by substitution, we can eliminate variables $t_i (i = 1, \ldots, 5)$ and obtain similarly

$$a^{q^5+q^4+q^3+q^2+q+1} + h_1 a^{q^4+q^3+q^2+q+1} + h_2 a^{q^3+q^2+q+1} + h_3 a^{q^2+q+1} + h_4 a^{q+1} + h_5 a = \beta \tag{3.10}$$

with $\beta \in \mathbb{F}_q$. As $h_i (i = 1, \ldots, 5)$ can be expressed in terms of g_1, g_2 and g_3, the equation (3.10) can be seen as a polynomial in a, u and g_3 as well. Choosing $\beta = \gamma = 1$ and computing the greatest common divisor of the resulting polynomials in equations (3.9) and (3.10) gives rise to an algebraic condition on a of degree three. As an aside, note that the choice

$\beta = \gamma = 1$ corresponds to finding a $\langle S+1, T+1\rangle$-isogeny. We obtain that the Drinfeld module ψ can be expressed in terms of u, g_3 and a. Now recall that l_1^3, l_2 and l_3^3 can also be expressed in some $v \in \mathbb{F}_{32}(l_2, l_3^3)$. It turns out that ψ does not correspond to a point in the same family of ϕ, but a conjugated one. In this case we need to apply Frobenius three times to go from the family to which the isomorphism class of ϕ belongs, to the family to which the isomorphism class of ψ belongs. Relating the parameters u and v we obtain that $\Phi(\alpha, u, v) = 0$ with

$$\begin{aligned}\Phi(\alpha, X, Y) := (X^3 + \alpha^{24}X^2 + \alpha^4 X + \alpha^9)Y^3 + (\alpha^{17}X^3 + \alpha^{29}X^2 + X + \alpha^{30})Y^2 \\ +(\alpha^{30}X^3 + \alpha^{12}X^2 + \alpha^{30}X + \alpha^{17})Y + (\alpha^4 X^3 + \alpha^{14}X^2 + \alpha^{19}).\end{aligned} \tag{3.11}$$

As noted before, the parameter u plays the same role as j_0 from Section 3.2. Similarly v plays the same role as j_1 and the polynomial $\Phi(\alpha, X, Y)$ can be seen as an analogue of a Drinfeld modular polynomial $\Phi_N(X, Y)$. For completeness, let us note that whereas N was a polynomial before, its role is now taken by the ideal $\langle S + 1, T + 1\rangle \subset A$ which implicitly played a role in the construction of the isogeny λ.

3.4.3 Obtaining a tower

Just as for the towers from Section 3.2, we need a quadratic extension of the constant field in order to obtain many rational places. From now on we will therefore work over the field $\mathbb{F}_{2^{10}}$ instead of $\mathbb{F}_{2^5}$. Let $\beta \in \mathbb{F}_{2^{10}}$ be a primitive element, the α's of the polynomial (3.11) should be changed in terms of β using the relation $\alpha = \beta^{33}$. We would now like to define a tower $\mathcal{F} := (F_0 \subset F_1 \subset \cdots)$ of function fields as follows:

$$F_0 := \mathbb{F}_{2^{10}}(u_0) \text{ and for } n \geq 0 \;\; F_{n+1} := F_n(u_{n+1}), \tag{3.12}$$

with $\Phi(\alpha^{8^n}, u_n, u_{n+1}) = 0$. There are two remarks to be made. In the first place, the reason one needs to take α^{8^n} as argument is that in the first iteration we went from one family of rank 2 Drinfeld modules to another (namely the one obtained by applying Frobenius three times). In the next iteration one therefore needs to start at this family. This amounts to replacing α by α^8 in equation (3.11). Iteratively in the $(n+1)$-th step we need to replace α by α^{8^n}. The second remark is that in fact

the polynomial $\Phi(\alpha^8, u_1, T) \in F_1[T]$ is not irreducible. It has the degree one factor $(u_0 + \alpha^{25})T + (\alpha^{28}u_0 + \alpha^{27})$ and a degree two factor. This is in perfect analogy with Proposition 3.1. To define the tower more accurately, we would have to specify this degree two factor and use that to define F_n if $n > 1$. A direct computation reveals there is always a totally ramified place with ramification index two in the extension F_{n+1}/F_n for $n > 0$ and hence that the degree two factor remains irreducible. This means that all the steps in the tower, except the first one, are Artin–Schreier extensions.

A careful analysis of the extension F_1/F_0 reveals the following:

Proposition 3.8. *The extension F_1/F_0 satisfies the following:*

1. $[F_1 : F_0] = 3$.
2. *The place $(u_0 = \beta^{858})$ is totally ramified; i.e., it has ramification index* 3.
3. *The places $(u_0 = \beta^{165}), (u_0 = \beta^{368}), (u_0 = \beta^{523})$, and $(u_0 = \beta^{891})$ are completely splitting.*
4. *Above each of the places $(u_0 = \beta^{198}), (u_0 = \beta^{330}), (u_0 = \beta^{528}), (u_0 = \beta^{627})$, and $(u_0 = \beta^{924})$ lie two places of F_1. One of these two has ramification index* 2 *and different exponent* 2*, the other has ramification index one.*
5. *The genus of F_1 is* 4.

Proof. All this follows by a direct computation, for example using Magma. □

The place mentioned, though ramified in the first extension turns out to split completely in all subsequent extensions. More precisely, denote by P the place of F_1 lying above $(u_0 = \beta^{858})$. Then one can show that P splits completely in any of the extensions F_n/F_1 for $n > 1$. Using the recursive structure of the tower $\mathcal{F}$, it is not hard to show this. Combining this with part (iii) of the above proposition, this yields the following:

Lemma 3.9. *Let $n > 0$. The number of rational places of F_n is at least $13 \cdot 2^{n-1}$.*

Also the genus of the function fields in the tower $\mathcal{F}$ can be estimated. Recall that F_{n+1}/F_n is an Artin–Schreier extension if $n > 0$. Using the recursive nature of the tower and either direct computation or a computer program like Magma, one can show that all ramification in the extension F_2/F_1 is 2-bounded, that is that for any place P of F_1 and any place Q of F_2 lying above F_1, we have $d(Q|P) = 2e(Q|P) - 2$. The same is true for the extension $F_2/\mathbb{F}_{2^{10}}(u_1, u_2)$. By [GS05, Lemma 1] and the recursive definition of the tower, this means that for any $n > 1$, the ramification in the extension F_n/F_1 is 2-bounded. By part (iv) of Proposition 3.8, there are exactly 10 places of F_1 that may ramify in F_n/F_1. Using Riemann–Hurwitz and the 2-boundedness of the ramification, we obtain for any $n > 1$ that

$$\begin{aligned} 2g(F_n) - 2 &= 2^{n-1}(2 \cdot 4 - 2) + \deg \operatorname{Diff}(F_n/F_1) \\ &\leq 2^{n-1}6 + 10 \cdot 2 \cdot 2^{n-1}. \end{aligned}$$

Hence we obtain the following:

Lemma 3.10. *For $n > 1$ we have $g(F_n) \leq 13 \cdot 2^{n-1} + 1$.*

This shows that the tower $\mathcal{F}$ is good. More precisely, we obtain from Lemmas 3.9 and 3.10 that:

$$\lambda(\mathcal{F}) \geq 1.$$

In other words, the tower defined by equation (3.12) is asymptotically good.

Chapter 4

Good families of Drinfeld modular curves

In this chapter we investigate examples of good and optimal Drinfeld modular towers of function fields. Surprisingly, the optimality of these towers has not been investigated in full detail in the literature. The current work can be seen as a continuation and solidification of the work started in Chapter 3 to explicitly define families of Drinfeld modular curves. We also give an algorithmic approach on how to obtain explicit defining equations for some of these towers and in particular give a new explicit example of an optimal tower over a quadratic finite field. Numerical experiments are presented in Appendix A. Apart from the introduction, the text of this chapter is kept as it was published in

[BBN15] A. Bassa, P. Beelen and N. Nguyen, *Good families of Drinfeld modular curves*, LMS Journal of Computation and Mathematics **18**, 699–712 (2015)

4.1 Preliminaries

To put this work into the right context of Drinfeld modular curves, we briefly recall some notions that we will use in the remainder of the chapter. Let $F/\mathbb{F}_q$ be a function field with full constant field $\mathbb{F}_q$ and let P be a place of degree d. Then we denote by F_P the residue field of P. It is a finite field with $|F_P| := q^d$ elements. For an integer $e \geq 1$, we denote by $F_P^{(e)}$ the algebraic extension of F_P of degree e. In the theory of Drinfeld modules and Drinfeld modular curves one singles out a place P_∞ of F (playing the role of a place at "infinity") and defines the ring A as the ring of all functions in F regular outside P_∞. We will denote the degree of P_∞ by δ.

For a non-zero monic polynomial $\mathfrak{n} \in \mathbb{F}_q[T]$ Gekeler investigates in [Gek79] (among other things) the Drinfeld modular curve $Y_0(\mathfrak{n})$. The points on this curve parametrize isomorphism classes of pairs of $\mathbb{F}_q[T]$-Drinfeld modules of rank 2 together with an $\mathfrak{n}$-isogeny between them. Adding so-called cusps gives a projective algebraic curve $X_0(\mathfrak{n})$ defined over F that in general however will not be absolutely irreducible. In case $\mathfrak{n} = 1$, the number of cusps is seen to be $(\delta \cdot h(F))^2$ while $X_0(1)$ has $\delta \cdot h(F)$ components [Gek86, VI.5]. Here $h(F)$ denotes the class number of the function field F. This implies that the number of absolutely irreducible components of $X_0(\mathfrak{n})$ equals $\delta \cdot h(F)$. Equivalently, the number of components is equal to $h(A)$, the cardinality of the ideal class group of the ring A. By considering the action of the ideal class group of A, one sees that the cusps are distributed equally among the absolutely irreducible components of $X_0(1)$, which implies that any such component contains exactly $\delta \cdot h(F)$ cusps. We will denote by $x_0(\mathfrak{n})$ an absolutely irreducible component of $X_0(\mathfrak{n})$. For any prime ideal of A (corresponding to a place of F different from P_∞), one obtains by reduction an algebraic curve defined over a finite field. In case of $A = \mathbb{F}_q[T]$ and $\delta = 1$, the curve $X_0(\mathfrak{n})$ (as well as its reduction modulo any prime P relatively prime to $\mathfrak{n}$) is absolutely irreducible. By computing the precise formula for the genus and the number of rational points on reductions of $\mathbb{F}_q[T]$-Drinfeld modular curves $X_0(\mathfrak{n})$, Gekeler [Gek04] showed that for a series $(\mathfrak{n}_k)_{k\in\mathbb{N}}$ of polynomials of A coprime with an irreducible polynomial $P \in A$, and whose degrees tend to infinity, the family of Drinfeld modular curves $X_0(\mathfrak{n}_k)/F_P$

attains the Drinfeld–Vladut bound when considered over $F_P^{(2)}$. In case $\mathfrak{n}_k = T^k$ and $P = T-1$, explicit equations for the modular curves $X_0(T^k)$ were given in [Elk98], while some more general examples (including defining equations in generic A-characteristic 0) were given in Chapter 3. For $A = \mathbb{F}_q[T]$ and $\delta = 1$ the situation has therefore to a large extent been investigated both theoretically and explicitly. However, we will see that generalizations to other rings A and values of δ are possible and that in some cases the resulting families of curves can be described by equations explicitly.

4.2 Genus calculation of $x_0(\mathfrak{n})$

In this section we will compute the genus of (an irreducible component of) the modular curve $X_0(\mathfrak{n})$. We put no restriction on the choice of function field F and place P_∞. A recipe for this genus computation is given in [Gek86] using results from [Gek79]. The recipe was carried out in [Gek86] in case $\mathfrak{n}$ is a prime ideal. We will in this section carry out the computations for any ideal $\mathfrak{n}$. The computations in [Gek79, Gek86] are carried out over the field C_∞, which is the completion of the algebraic closure of the completion of F at P_∞. For our purposes one therefore needs to check that the genus of $x_0(\mathfrak{n})$ does not change when changing the constant field. For $A = \mathbb{F}_q[T]$, this result is contained in [Sch97]. In our case, note that the only points that ramify in the cover $X(\mathfrak{n})/X(1)$ are the elliptic points of $X(1)$ and the cusps of $X(1)$. The residue field of a cusp is isomorphic to the Hilbert class field of F [Gek86, Thm. 1.9 (ii), p.81], while the residue field of an elliptic point is a subfield of the Hilbert class field of $\mathbb{F}_{q^2}F$ [Gek86, Prop. 2.2, p.83]. In either case, the residue field is a separable extension of the field F. Using Corollary 3.4.2 from [Gol03], we see that the argument given in [Sch97] carries over to our situation.

One of the ingredients in the genus expressions of $x_0(\mathfrak{n})$ involve the L-polynomial of the function field F, which we will denote by $P(t)$. Note that $P(1) = h(F)$, the class number of F. The following functions will also be useful:

Definition 4.1. Let $\mathfrak{n} \subset A$ be an ideal and suppose that $\mathfrak{n} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_s^{r_s}$,

for prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ and positive integers $r_1, \ldots, r_s$. Writing $q_i := |\mathfrak{p}_i| = |A/\mathfrak{p}_i|$, we define

$$\varphi(\mathfrak{n}) := |(A/\mathfrak{n})^*| = \prod_{i=1}^{s} q_i^{r_i-1}(q_i - 1),$$

$$\varepsilon(\mathfrak{n}) := \prod_{i=1}^{s} q_i^{r_i-1}(q_i + 1).$$

and

$$\kappa(\mathfrak{n}) := \prod_{i=1}^{s} (q_i^{[r_i/2]} + q_i^{r_i-[r_i/2]-1}),$$

where $[r]$ denotes the integral part of a real number r.

Using these notions, we will obtain that

Theorem 4.2. *Let A and $\mathfrak{n}$ be as above. In particular suppose that $\mathfrak{n} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_s^{r_s}$, for prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ and positive integers $r_1, \ldots, r_s$. Then we have*

$$g(x_0(\mathfrak{n})) = 1 + \frac{(q^\delta - 1)\varepsilon(\mathfrak{n})P(q)}{(q^2-1)(q-1)} - \frac{P(1)\delta(\kappa(\mathfrak{n}) + 2^{s-1}(q-2))}{q-1} + \eta,$$

where $\eta = -P(-1)2^{s-1}q/(q+1)$ if δ is odd and all prime divisors of $\mathfrak{n}$ are of even degree, $\eta = 0$ otherwise.

Note that [Gek86, VII. 5.13] (the case that $\mathfrak{n}$ is a prime ideal) is a special case of this theorem.

The recipe outlined in [Gek86] consists of the following ingredients: first compute the genus of $x_0(1)$, then consider the cover $x_0(\mathfrak{n})/x_0(1)$. Since (like in the case of classical modular curves) this cover is not Galois in general, one studies a Galois cover $x(\mathfrak{n})/x_0(1)$ first. The curve $x(\mathfrak{n})$ is an irreducible component of the modular curve $X(\mathfrak{n})$, whose points correspond to isomorphism classes of A-Drinfeld modules ϕ of rank 2 together with an isomorphism of $\phi[\mathfrak{n}]$ with $(A/\mathfrak{n})^2$. Note that $X_0(1) = X(1)$ and that the points on this curve correspond to isomorphism classes of A-Drinfeld modules of rank 2.

Since $x(\mathfrak{n})/x(1)$ is Galois, so is $x(\mathfrak{n})/x_0(\mathfrak{n})$. The Galois group of the cover $x(\mathfrak{n})/x(1)$, resp. $x(\mathfrak{n})/x_0(\mathfrak{n})$, is given by $G(\mathfrak{n})$, resp. $H(\mathfrak{n})$ defined as [Gek86, VII.5]:

$$G(\mathfrak{n}) := \{\gamma \in \mathrm{GL}(2, A/\mathfrak{n}) : \det\gamma \in \mathbb{F}_q^*\}/Z(\mathbb{F}_q)$$

and

$$H(\mathfrak{n}) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}(2, A/\mathfrak{n}) : ad \in \mathbb{F}_q^* \right\} /Z(\mathbb{F}_q),$$

with

$$Z(\mathbb{F}_q) := \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{F}_q^* \right\}.$$

Before proceeding, we calculate the cardinalities of the groups $G(\mathfrak{n})$ and $H(\mathfrak{n})$. The latter cardinality is relatively easy, since in that case $a \in (A/\mathfrak{n})^*$ and $b \in A/\mathfrak{n}$ can be chosen freely (leaving $q-1$ possibilities for d). Therefore, we have

$$|H(\mathfrak{n})| = |(A/\mathfrak{n})^*| \cdot (q-1) \cdot |A/\mathfrak{n}|/(q-1) = \varphi(\mathfrak{n})|\mathfrak{n}|. \tag{4.1}$$

To count the cardinality of $G(\mathfrak{n})$, observe that

$$|\mathrm{SL}(2, A/\mathfrak{n})| = \frac{|\{\gamma \in \mathrm{GL}(2, A/\mathfrak{n}) : \det\gamma \in \mathbb{F}_q^*\}|}{q-1},$$

since any nonzero value in $\mathbb{F}_q$ of the determinant is taken equally often when considering elements in $\{\gamma \in \mathrm{GL}(2, A/\mathfrak{n}) : \det\gamma \in \mathbb{F}_q^*\}$. By definition of $G(\mathfrak{n})$, we obtain that

$$|G(\mathfrak{n})| = |\mathrm{SL}(2, A/\mathfrak{n})|.$$

The cardinality of $\mathrm{SL}(2, A/\mathfrak{n})$ is well known and can be computed using the Chinese remainder theorem. This approach gives that if $\mathfrak{n} = \prod_i \mathfrak{p}_i^{r_i}$ for prime ideals $\mathfrak{p}_i \subset A$, then

$$|\mathrm{SL}(2, A/\mathfrak{n})| = \prod_i |\mathrm{SL}(2, A/\mathfrak{p}_i^{r_i})| = \prod_i |\mathfrak{p}_i|^{3r_i-2}(|\mathfrak{p}_i|^2 - 1) = \varphi(\mathfrak{n})\varepsilon(\mathfrak{n})|\mathfrak{n}|,$$

implying that

$$|G(\mathfrak{n})| = \varphi(\mathfrak{n})\varepsilon(\mathfrak{n})|\mathfrak{n}|. \tag{4.2}$$

We now turn our attention again to the Galois cover $x(\mathfrak{n})/x(1)$. It was shown in [Gek86] that the only ramification in this cover occurs above

the so-called elliptic points (with ramification index $q+1$) and the cusps of $x(1)$. Moreover, as mentioned before, the number of cusps on $x(1)$ equals $\delta h(F)$. The elliptic points were studied in [Gek86, V.4,VII.5]: The number of elliptic points on $x(1)$ is 0 if δ is even and $P(-1)$ if δ if odd, each with ramification index $q+1$ in the cover $x(\mathfrak{n})/x(1)$. We now write, just as before, $\mathfrak{n} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_s^{r_s}$ for prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of A and positive integers $r_1, \ldots, r_s$. Although $x(1)$ contains $P(-1)$ elliptic points if δ is odd, such an elliptic point does not give rise to ramification in the cover $x(\mathfrak{n})/x_0(\mathfrak{n})$ if any of the $\mathfrak{p}_i$ has odd degree. If δ is odd and all prime ideals $\mathfrak{p}_i$ occurring in the decomposition of $\mathfrak{n}$ have even degree, among all the points of $x_0(\mathfrak{n})$ that are lying above a given elliptic point of $x(1)$ there are exactly 2^s that are ramified in the covering $x(\mathfrak{n})/x_0(\mathfrak{n})$ (with ramification index $q+1$). This completely determines the behaviour of elliptic points as far as their role in the genus computation of $x(\mathfrak{n})$ and $x_0(\mathfrak{n})$ goes. To describe the behaviour of the cusps, we start by describing their ramification groups in $x(\mathfrak{n})/x(1)$ (following [Gek86, VII.5]):

Lemma 4.3 (Lemma 5.6 [Gek86])**.** *Let*

$$G(\mathfrak{n})_\infty := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}(2, A/\mathfrak{n}) : a, d \in \mathbb{F}_q^* \right\} / Z(\mathbb{F}_q).$$

Then the stabilizers of all cusps of $x(\mathfrak{n})$ are conjugate in $G(\mathfrak{n})$ to $G(\mathfrak{n})_\infty$.

This means in particular that the ramification index in $x(\mathfrak{n})/x(1)$ of any cusp equals $|G(\mathfrak{n})_\infty| = (q-1)^2|\mathfrak{n}|/(q-1) = (q-1)|\mathfrak{n}|$. The cardinality of the first, resp. second, ramification group of any cusp is then calculated in [Gek86, Lemma 5.7] to be $|\mathfrak{n}|$, resp. 1. This means that the different exponent for a cusp equals $(q-1)|\mathfrak{n}| - 1 + |\mathfrak{n}| - 1 = q|\mathfrak{n}| - 2$. Combining this information concerning the ramification groups of the cusps with the description of the ramification behaviour of the elliptic points, makes the computation of the genus of $x(\mathfrak{n})$ completely feasible using the Riemann–Hurwitz genus formula. The result (given in slightly less explicit form in [Gek86, Theorem 5.11]) is:

$$g(x(\mathfrak{n})) = 1 + \frac{(q^\delta - 1)P(q)}{(q^2-1)(q-1)}\varphi(\mathfrak{n})\varepsilon(\mathfrak{n})|\mathfrak{n}| - \frac{\delta P(1)}{q-1}\varphi(\mathfrak{n})\varepsilon(\mathfrak{n}). \qquad (4.3)$$

The ramification behaviour of the cusps is more complicated in the cover $x(\mathfrak{n})/x_0(\mathfrak{n})$. However, in [Gek86, VII.5] (with reference to [Gek79, 3.4.15])

the total contribution to the Riemann–Hurwitz genus formula for the cover $x(\mathfrak{n})/x_0(\mathfrak{n})$ of all cusps of $x(\mathfrak{n})$ lying above a single cusp of $x(1)$ is computed to be

$$(q-1)^{-1}\varphi(\mathfrak{n})(2|\mathfrak{n}|\kappa(\mathfrak{n}) + 2^s(q-2)|\mathfrak{n}| - 2\varepsilon(\mathfrak{n})). \tag{4.4}$$

We now have all the ingredients needed for the proof of Theorem 4.2

Proof. For any point P of $x(\mathfrak{n})$, we denote by $e(P)$, resp. $d(P)$, the ramification index, resp. different exponent, in the cover $x(\mathfrak{n})/x_0(\mathfrak{n})$. Since the only ramified points in the cover $x(\mathfrak{n})/x(1)$ are the cusps and the elliptic points (if these exist), applying the Riemann–Hurwitz genus formula for the cover $x(\mathfrak{n})/x_0(\mathfrak{n})$ we obtain:

$$2g(x(\mathfrak{n})) - 2 = \varphi(\mathfrak{n})|\mathfrak{n}|(2g(x_0(\mathfrak{n})) - 2) + \sum_{P \text{ cusp}} d(P) + \sum_{\substack{P \text{ elliptic} \\ \text{point}}} d(P). \tag{4.5}$$

The sum concerning the elliptic points is zero if no such points exist and therefore:

$$\sum_{\substack{P \text{ elliptic} \\ \text{point}}} d(P) = 0,$$

if δ is even or if there exists $\mathfrak{p}_i$ of odd degree. Otherwise, as we have described previously, above each of the $P(-1)$ cusps of $x(1)$ lie exactly 2^s points of $x_0(\mathfrak{n})$ that ramify with ramification index $q+1$ in $x(\mathfrak{n})/x_0(\mathfrak{n})$. This implies that

$$\sum_{\substack{P \text{ elliptic} \\ \text{point}}} d(P) = \sum_{\substack{P \text{ elliptic} \\ \text{point}}} q = P(-1)2^s q|\mathfrak{n}|\varphi(\mathfrak{n})/(q+1),$$

if δ is odd and all prime divisors of $\mathfrak{n}$ have even degree.

The summation over the points lying over any of the $\delta h(F)$ cusps of $x(1)$ can be dealt with using Equation (4.4). We obtain that

$$\sum_{P \text{ cusp}} d(P) = \delta h(F)(q-1)^{-1}\varphi(\mathfrak{n})(2|\mathfrak{n}|\kappa(\mathfrak{n}) + 2^s(q-2)|\mathfrak{n}| - 2\varepsilon(\mathfrak{n})).$$

Substituting these values in Equation (4.5) and using Equation (4.3), Theorem 4.2 follows. □

4.3 Rational points on reductions of Drinfeld modular curves

In this section, we combine the previously described genus computation of the curves $x_0(\mathfrak{n})$ with the fact that reductions of these curves have many rational points (when the field of definition is chosen properly). We will show that for any sequence of ideals $(\mathfrak{n}_k)_{k\geq 1}$ such that $\deg \mathfrak{n}_k \to \infty$ as $k \to \infty$, the corresponding family of reductions of Drinfeld modular curves $(x_0(\mathfrak{n}_k))_k$ has good asymptotic properties. In [Tae06] the (reductions of the) curves $x_0(\mathfrak{n})$ were also investigated in case $\mathfrak{n}$ is a principal ideal, using a different method inspired by [Iha81]. Our approach is to use, for any ideal $\mathfrak{n}$, results from [Gek90] to estimate the number of rational points on the reduction of $x_0(\mathfrak{n})$ and to use the explicit genus formula for $g(x_0(\mathfrak{n}))$ from the previous section.

While the curves $X_0(\mathfrak{n})$ themselves are defined over the function field F (and a component $x_0(\mathfrak{n})$ over an extension field of F), a model can be found that can be reduced modulo prime ideals of the ring A. This reduction is known to be good if $P \subset A$ is a prime ideal which is coprime with the ideal $\mathfrak{n}$. Thus, reduction modulo P gives rise to a curve (as before not necessarily absolutely irreducible) that is defined over the finite field A/P. For convenience we write $F_P := A/P$ and denote by $F_P^{(m)}$ the degree m extension of F_P. In case $A = \mathbb{F}_q[T]$, these reduced Drinfeld modular curves have many rational points over $F_P^{(2)}$ (essentially corresponding to supersingular A-Drinfeld modules), but it turns out that in general the situation is slightly more complicated. As a matter of fact the supersingular Drinfeld modules in A-characteristic P are in general defined over the field $F_P^{(2e)} = \mathbb{F}_{q^{2de}}$ with $d = \deg P$ and $e = \operatorname{ord} P$, the order of the ideal P in the ideal class group of the ring A [Gek90, Section 4].

More precisely, in [Gek90] it was shown that for a prime ideal $P \subset A$ with $d := \deg P$, the number $N(P)$ of isomorphism classes of supersingular A-Drinfeld modules in A-characteristic P equals $N(P) = h_1(P) + h_2(P)$

with

$$h_1(P) := \begin{cases} \delta P(1)\left(P(q)\frac{(q^\delta-1)(q^d-1)}{(q^2-1)(q-1)} - \frac{P(-1)}{q+1}\right), & \text{if } d \text{ and } \delta \text{ are odd,} \\ \\ \delta P(1)P(q)\frac{(q^\delta-1)(q^d-1)}{(q^2-1)(q-1)} & \text{otherwise,} \end{cases} \tag{4.6}$$

and

$$h_2(P) := \begin{cases} \delta P(1)P(-1), & \text{if } d \text{ and } \delta \text{ are odd,} \\ \\ 0 & \text{otherwise.} \end{cases} \tag{4.7}$$

Each isomorphism class of a supersingular A-Drinfeld module gives rise to a rational point (which we will call a supersingular point) on the curve $X(1)$, if the field of definition is taken to be $F_P^{(2e)}$. Using the action given by the class group of A on the absolutely irreducible components of $X(1)$, one sees that the supersingular points are equidistributed among all $\delta P(1)$ components of $X(1)$. These observations enable us to give a lower bound on the number of rational points on $x_0(\mathfrak{n})$:

Theorem 4.4. *Let $\mathfrak{n} \subset A$ be an ideal prime to the A-characteristic P and suppose that $\mathfrak{n} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_s^{r_s}$, for prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ and positive integers $r_1, \ldots, r_s$. Moreover, denote by $d := \deg P$ and $e := \operatorname{ord} P$. Consider over the finite field $F_P^{(2e)}$ a component $x_0(\mathfrak{n})$ of $X_0(\mathfrak{n})$ and denote by $N_1(x_0(\mathfrak{n}))$ its number of rational points. Then if d, δ are odd, and $\deg \mathfrak{p}_i$ is even for all i, we have*

$$N_1(x_0(\mathfrak{n})) \geq \varepsilon(\mathfrak{n})P(q)\frac{(q^\delta-1)(q^d-1)}{(q^2-1)(q-1)} + P(-1)2^s\frac{q}{q+1},$$

while otherwise

$$N_1(x_0(\mathfrak{n})) \geq \varepsilon(\mathfrak{n})P(q)\frac{(q^\delta-1)(q^d-1)}{(q^2-1)(q-1)}.$$

Proof. All points of $x_0(\mathfrak{n})$ lying above one of the $N(P)/(\delta P(1))$ supersingular points of $x(1)$ are rational, but not necessarily unramified in the covering $x_0(\mathfrak{n})/x(1)$. The reason for this is that the elliptic points are supersingular points if (and only if) both δ and d are odd [Gek90, Lemma 7.2]. However, any elliptic point has ramification index either one, or $q+1$ in the cover $x_0(\mathfrak{n})/x(1)$. Moreover, from [Gek86, V.4,VII.5] we see

that if δ is odd and all prime ideals $\mathfrak{p}_i$ occurring in the decomposition of $\mathfrak{n}$ have even degree, among all the points of $x_0(\mathfrak{n})$ that are lying above a given elliptic point of $x(1)$ there are exactly 2^s that are ramified in the covering $x(\mathfrak{n})/x_0(\mathfrak{n})$ (with ramification index $q+1$). The latter statement is equivalent to saying that these 2^s points of $x_0(\mathfrak{n})$ have ramification index 1 in $x_0(\mathfrak{n})/x(1)$. Counting the number of points of $x_0(\mathfrak{n})$ lying above the supersingular points of $x(1)$ now is direct and yields the stated lower bound on $N_1(x_0(\mathfrak{n}))$. □

From Theorem (4.2) we get the following asymptotic result:

Theorem 4.5. *Let A be any ring of functions regular outside a fixed place ∞ of degree δ. Let $P \subset A$ be a prime ideal of degree d and order e and further let $(\mathfrak{n}_k)_{k\geq 1}$ be a series of ideals relatively prime to P. The family of reductions of Drinfeld modular curves $(x_0(\mathfrak{n}_k))_k$ when defined over $\mathbb{F}_{q^{2de}}$ satisfies*

$$\lim_{k\to\infty} \frac{N_1(x_0(\mathfrak{n}_k))}{g(x_0(\mathfrak{n}_k))} \geq q^d - 1.$$

Remark 4.6. The lower bound given in Theorem 4.5 is sharp in case P is a principal ideal, since in this case $e = 1$ and the given lower bound is equal to the Drinfeld–Vladut upper bound. If $A = \mathbb{F}_q[T]$ (in particular $\delta = 1$), the ideal class group of A is trivial, implying that any family of reductions of Drinfeld modular curves as in Theorem 4.5 has optimal asymptotic properties. This particular case was shown in [Gek04]. If P is not principal, the resulting families will be asymptotically good, but not optimal. Note that in [Tae06] this subtlety is missing.

4.4 A recursive description of a Drinfeld modular tower

In this section we will illustrate Theorem 4.5 by describing some families of Drinfeld modular curves $(x_0(\mathfrak{n}_k))_k$ more explicitly. In case $\mathfrak{n}_k = \mathfrak{p}^k$ for a fixed prime ideal $\mathfrak{p}$ of A, this can be done in a recursive way (in fact $\mathfrak{p}$ could be any non-trivial ideal, but we will assume primality for

simplicity). The reason for this is similar to the reasoning presented in [Elk98, Elk01], but is somewhat more involved due to the fact that the curves $X(1)$ and $X_0(\mathfrak{p}^k)$ are not absolutely irreducible in general. Therefore, we go through the argument in the following.

A point on $X_0(\mathfrak{p})$ corresponds to an isomorphism class $[\phi, \psi]$ of a pair of $\mathfrak{p}$-isogenous A-Drinfeld modules of rank 2. Therefore, there are two possible maps, say π_1 and π_2, from $X_0(\mathfrak{p})$ to $X(1)$, see Figure 4.1, since one can send $[\phi, \psi]$ to $[\phi]$ or $[\psi]$ (the isomorphism class of ϕ or that of ψ). Since a $\mathfrak{p}$-isogeny corresponds to a cyclic submodule of the $\mathfrak{p}$-torsion points of ϕ, the degree of the first map is $|\mathfrak{p}|+1$. By symmetry, the degree of the second map is also $|\mathfrak{p}| + 1$.

The image of a fixed absolutely irreducible component $x_0(\mathfrak{p})$ of $X_0(\mathfrak{p})$ under either π_1 or π_2, will be an absolutely irreducible component of $X(1)$, but not necessarily the same one. We denote these components by $x^1(1)$ and $x^2(1)$. We can then view $x_0(\mathfrak{p})$ as a curve lying inside $x^1(1) \times x^2(1)$. Once an explicit description of the components of $x^1(1)$ and $x^2(1)$ is available, the map $\pi_1 \times \pi_2 : x_0(\mathfrak{p}) \to x^1(1) \times x^2(1)$ defined by $[\phi, \psi] \mapsto ([\phi], [\psi])$, can be in principle be used to describe the curve $x_0(\mathfrak{p})$ explicitly by equations. However, in practice it is very convenient to assume that the genera of the components of $X(1)$ are zero. In this case, a component $x^i(1)$ can just be described using a single variable u_i, which one can think of as a j-invariant of an A-Drinfeld module. In this case a component of $X_0(\mathfrak{p})$ can be described using a bivariate polynomial $\Phi(u_1, u_2)$ of bi-degree $(|\mathfrak{p}|+1, |\mathfrak{p}|+1)$ (that is, of degree $|\mathfrak{p}|+1$ in either of the two variables u_1 and u_2). Note that for $\mathfrak{n} = 1$, Equation (4.3) states that

$$g(x(1)) = 1 + (q^2 - 1)^{-1} \left(\frac{q^\delta - 1}{q - 1} P(q) - \frac{q(q+1)}{2} \delta P(1) + \eta \right), \quad (4.8)$$

where $\eta = -q(q-1)P(-1)/2$ for δ odd, $\eta = 0$ otherwise. As a matter of fact, this formula was stated in [Gek86, VI.5.8] and was used as a key ingredient there to showing Equation (4.3). Using Equation (4.8), one readily sees that $g(x(1)) = 0$ if $F = \mathbb{F}_q(T)$ and $\delta \in \{1, 2, 3\}$ or if F is the function field of an elliptic curve and $\delta = 1$. For simplicity, we assume from now on that we are in one of these situations, though the general considerations below remain valid in the general case as well. However,

finding explicit equations is only possible if (the function field of) the curve $x(1)$ can be given explicitly, which is trivial if it has genus zero.

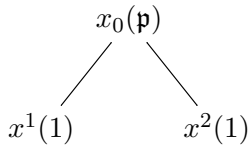

Figure 4.1: A correspondence of modular curves.

A description of $x_0(\mathfrak{p}^2)$ (a component of $X_0(\mathfrak{p}^2)$) can now be obtained relatively easily. A point on $X_0(\mathfrak{p}^2)$ corresponds to an isomorphism class $[\phi_1, \phi_3]$ of a pair of $\mathfrak{p}^2$-isogenous A-Drinfeld modules of rank 2. Let $\mu : \phi_1 \to \phi_3$ be the corresponding $\mathfrak{p}^2$-isogeny. Then there exists a A-Drinfeld module ϕ_2 of rank 2 and $\mathfrak{p}$-isogenies $\lambda_1 : \phi_1 \to \phi_2$ and $\lambda_2 : \phi_2 \to \phi_3$ such that $\mu = \lambda_2 \circ \lambda_1$. The isomorphism class of $[\phi_i]$ will correspond to a point on a component $x^i(1)$ of $X(1)$. This means that we can map $x_0(\mathfrak{p}^2)$ to $x^1(1) \times x^2(1) \times x^3(1)$. Note that both $[\phi_1, \phi_2]$ and $[\phi_2, \phi_3]$ correspond to points on $X_0(\mathfrak{p})$, lying on certain components, say $x_0^1(\mathfrak{p})$ and $x_0^2(\mathfrak{p})$. Using the above procedure, we can describe these two components as the zero set of polynomials $\Phi^1(u_1, u_2)$ and $\Phi^2(u_2, u_3)$, both of bi-degree $(|\mathfrak{p}| + 1, |\mathfrak{p}| + 1)$. This means that image of the map from $x_0(\mathfrak{p}^2)$ to $x^1(1) \times x^2(1) \times x^3(1)$ is part of the zero set of the polynomials $\Phi^1(u_1, u_2)$ and $\Phi^2(u_2, u_3)$. However, this zero set turns out to be too large. The reason for this is that if (ϕ_1, ϕ_2) and (ϕ_2, ϕ_3) are two pairs of $\mathfrak{p}$-isogenous A-Drinfeld modules of rank 2, with $\mathfrak{p}$-isogenies denoted by λ_1 and λ_2, then $\lambda_2 \circ \lambda_1$ is either a $\mathfrak{p}^2$-isogeny, or has kernel isomorphic to $A/\mathfrak{p} \times A/\mathfrak{p}$. Here we used that $\mathfrak{p}$ is a prime ideal. The latter case gives rise to additional elements in the zero set of $\Phi^1(u_1, u_2)$ and $\Phi^2(u_2, u_3)$. However, this issue is rather easy to resolve: We work over the function field of $x_0^1(\mathfrak{p})$, which we can construct using the polynomial $\Phi^1(u_1, u_2)$. The polynomial $\Phi^2(u_2, u_3)$, viewed as a univariate polynomial in u_3 and coefficients in the function field of $x_0^1(\mathfrak{p})$, has degree $|\mathfrak{p}| + 1$ in u_3 while the extension degree of $X_0(\mathfrak{p}^2)/X(1)$ is $\varepsilon(\mathfrak{p}^2) = (|\mathfrak{p}| + 1)|\mathfrak{p}|$. Then the polynomial $\Phi^2(u_2, u_3)$ is not absolutely irreducible and has a (for degree reasons necessarily unique) component of degree $|\mathfrak{p}|$ in u_3. This component can then be used to construct (the function field of) $x_0(\mathfrak{p}^2)$, also see Figure 4.2.

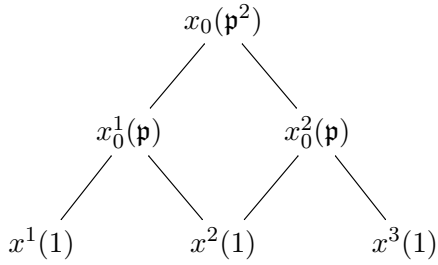

Figure 4.2: Recursive description of $x_0(\mathfrak{p}^2)$.

Iterating this procedure gives rise to an explicit recursive description of $x_0(\mathfrak{p}^k)$ for any $k \geq 1$. One effectively just increases the size of the pyramid in Figures 4.1 and 4.2. Note that since $X(1)$ only has finitely many absolutely irreducible components, ultimately the same components will start to occur, see Figure 4.3.

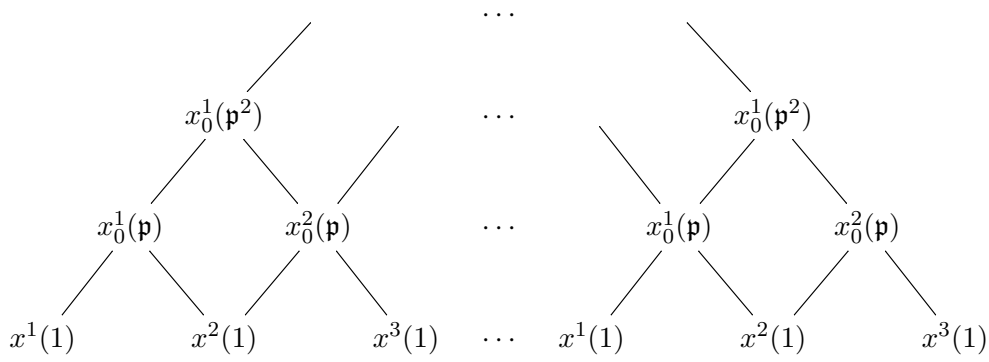

Figure 4.3: The pyramid of Drinfeld modular curves.

In case $A = \mathbb{F}_q[T]$, $\delta = 1$, $\mathfrak{p} = T$ and A-characteristic $T - 1$, explicit equations were found in [Elk98]. In this case all curves $X(1), X_0(\mathfrak{p}^k)$ are absolutely irreducible, so there is no need to keep track of components or to distinguish between $X_0(T^k)$ and one of its components $x_0(T^k)$. The curve $X_0(T)$ can be described using the Drinfeld modular polynomial $\Phi_T(u_1, u_2)$. However, the approach in [Elk98] exploits the fact that the genera of the curves $X_0(T)$ and $X_0(T^2)$ are zero. Compared to our ap-

proach this means that the "pyramid" in Figure 4.3 starts at $X_0(\mathfrak{p}^2)$, but otherwise the recursive description is similar: The points on the curve $X_0(T^k)$ are identified with points in $X_0(T^2) \times \cdots \times X_0(T^2)$, while each of the component curves $X_0(T^2)$ can be described using a single parameter v_i. For more details see [Elk98, BBN14].

4.5 An new explicit example of an optimal Drinfeld modular tower

In Chapter 3 some examples of good towers were found following the above approach, including one where the function field F was the function field of an elliptic curve and $\delta = 1$. More precisely, in the latter example in Chapter 3 one had $F = \mathbb{F}_2(X, Y)$ with X transcendental over $\mathbb{F}_2$ and $Y^2 + Y = X^3 + X$, while "infinity" was chosen to be the place at infinity of this elliptic curve, implying that $\delta = 1$. The ring A is then easily seen to be $\mathbb{F}_2[X, Y] \cong \mathbb{F}_2[T, S]/\langle S^2 + S + T^3 + T \rangle$. A description was given of the tower $X_0(\mathfrak{p}^k)$ with $\mathfrak{p} := \langle X + 1, Y + 1 \rangle \subset A$ and A-characteristic $P := \langle X, Y \rangle$. Note that $\deg P = 1$, since P is a rational point on the elliptic curve, and $\operatorname{ord} P = 5$, since the elliptic curve has 5 rational points, meaning that the group of rational points is cyclic of order 5. It was shown in Chapter 3 by explicit computation that the tower $X_0(\mathfrak{p}^k)$ (in A-characteristic $\langle T, S \rangle$) has limit at least 1 when the constant field is set to $\mathbb{F}_{2^{10}}$. This result is confirmed by Theorem 4.2. In this section we will in a similar way as in Chapter 3 describe an explicit example of an optimal tower. Contrary to the example referred to above and motivated by Theorem 4.2, the choice of A-characteristic P is now made such that $\operatorname{ord} P = 1$, implying that the resulting tower is optimal. The point with this example is not to give another optimal tower, but to show an explicit description is within reach. Such a description is useful for applications in for example coding theory.

More precisely, we will consider the following setting:

1. $F/\mathbb{F}_q := \mathbb{F}_2(X, Y)/\mathbb{F}_2$, where $Y^2 + XY + X^2 = X$ and X is transcendental over $\mathbb{F}_2$.

2. $A := \mathbb{F}_2[X, Y]$, implying $\delta = 2$.

3. The A-characteristic P is the principal prime ideal $\langle X^2 + X + 1 \rangle \subset A$.

Note that the function field F has genus 0, implying that the L-polynomial $P(t)$ occurring in the zeta function of F is simply $P(t) = 1$. Therefore the curve $X(1)$ has $\delta P(1) = 2$ absolutely irreducible components, say $x^1(1)$ and $x^2(1)$ both of genus 0 according to Equation 4.8. Since for the given choice of P we have $\operatorname{ord} P = 1$ (since P is a principal ideal) and $\deg P = 4$, Theorem 4.2 implies that, for any choice of prime ideal $\mathfrak{p} \subset A$ coprime with the A-characteristic P, the limit of the resulting family of curves $(X_0(\mathfrak{p}^k))_k$ when defined over the finite field $\mathbb{F}_{2^8}$ equals $\sqrt{2^8} - 1 = 15$. In other words, the resulting family of curves is optimal over $\mathbb{F}_{2^8}$.

We start by indicating how to describe A-Drinfeld modules explicitly. An A-Drinfeld module of rank 2 is symbolically determined by

$$\begin{aligned} \phi_X &= g_0\tau^4 + g_1\tau^3 + g_2\tau^2 + g_3\tau + \iota(X), \\ \phi_Y &= h_0\tau^4 + h_1\tau^3 + h_2\tau^2 + h_3\tau + \iota(Y). \end{aligned}$$

Since we have chosen the principal prime ideal $\langle X^2 + X + 1 \rangle$ as A-characteristic, we have $\iota(X)^2 + \iota(X) + 1 = 0$ and, using the equation of the curve, $\iota(Y)^2 + \iota(X)\iota(Y) + \iota(X)^2 = \iota(X)$. For convenience we will write

$$x := \iota(X) \quad \text{and} \quad y := \iota(Y).$$

We see that $x = \iota(X) \in \mathbb{F}_4$ and $y = \iota(Y) \in \mathbb{F}_{16}$. The remaining coefficients also satisfy several algebraic relations, stemming from the fact that $\phi_X\phi_Y = \phi_Y\phi_X$ and $\phi_{Y^2+XY+X^2-X} = 0$. Indeed, any choice of $g_0, \ldots, h_3$ satisfying these relations gives rise to a Drinfeld module. The equation

$\phi_X\phi_Y = \phi_Y\phi_X$ implies that:

$$g_0 h_0^{q^4} = h_0 g_0^{q^4} \tag{4.9}$$

$$g_0 h_1^{q^4} + g_1 h_0^{q^3} = h_0 g_1^{q^4} + h_1 g_0^{q^3} \tag{4.10}$$

$$g_0 h_2^{q^4} + g_1 h_1^{q^3} + g_2 h_0^{q^2} = h_0 g_2^{q^4} + h_1 g_1^{q^3} + h_2 g_0^{q^2} \tag{4.11}$$

$$g_0 h_3^{q^4} + g_1 h_2^{q^3} + g_2 h_1^{q^2} + g_3 h_0^{q} = h_0 g_3^{q^4} + h_1 g_2^{q^3} + h_2 g_1^{q^2} + h_3 g_0^{q} \tag{4.12}$$

$$g_1 h_3^{q^3} + g_2 h_2^{q^2} + g_3 h_1^{q} + x h_0 = h_0 x^{q^4} + h_1 g_3^{q^3} + h_2 g_2^{q^2} + h_3 g_1^{q} \tag{4.13}$$

$$g_1 y^{q^3} + g_2 h_3^{q^2} + g_3 h_2^{q} + x h_1 = h_1 x^{q^3} + h_2 g_3^{q^2} + h_3 g_2^{q} + y g_1 \tag{4.14}$$

$$g_2 y^{q^2} + g_3 h_3^{q} + x h_2 = h_2 x^{q^2} + h_3 g_3^{q} + y g_2 \tag{4.15}$$

$$g_3 y^{q} + x h_3 = h_3 x^{q} + y g_3 \tag{4.16}$$

Note that throughout this section we assume that $q = 2$. Similarly the equation $\phi_{Y^2+XY+X^2-X} = 0$ gives rise to algebraic relations. From Equations (4.16), (4.15) and (4.14), one sees that the three variables g_3, g_2, g_1 can be expressed in the three variables h_3, h_2, h_1. After eliminating g_1, g_2, g_3 in this way, Equations (4.13), (4.12), (4.11), (4.10) give rise to pairs of polynomials in h_1. These polynomials turn out to have a very special form: they are linearized polynomials in h_1 plus a constant term. Therefore, we can use the q-linearized variant of the Euclidean algorithm to eliminate the variable h_1 very efficiently, thus avoiding a lengthy Groebner basis computation. Finally we may use Equation (4.9) to normalize the leading coefficients g_0 and h_0 by putting $h_0 = 1$ and choosing $g_0 \in \mathbb{F}_4$ such that $g_0^2 + g_0 + 1 = 0$. We are then left with an explicit algebraic equation relating h_2 and h_3, say $f(h_2, h_3) = 0$, with coefficients in $\mathbb{F}_{16}$. The equation is a bit lengthy, but we state it for the

sake of completeness:

$$
\begin{aligned}
f(h_2,h_3) = {} & h_2^{30} + (xy+x)h_2^{29}h_3^3 + (y+x)h_2^{27}h_3^9 + (xy+1)h_2^{26}h_3^{12} + (y+1)h_2^{25} \\
& + (xy+x)h_2^{24}h_3^{18} + (x^2y+x^2)h_2^{24}h_3^3 + yh_2^{23}h_3^{21} + (x^2y+1)h_2^{23}h_3^6 + x^2yh_2^{22}h_3^9 \\
& + (xy+1)h_2^{21}h_3^{27} + (x^2y+x)h_2^{21}h_3^{12} + h_2^{20}h_3^{30} + (y+1)h_2^{20}h_3^{15} + (xy+1)h_2^{20} \\
& + (x^2y+x^2)h_2^{19}h_3^{18} + yh_2^{18}h_3^{36} + (xy+x)h_2^{18}h_3^6 + (y+x)h_2^{17}h_3^{39} + (y+x^2)h_2^{17}h_3^{24} \\
& + xh_2^{17}h_3^9 + (x^2y+1)h_2^{16}h_3^{27} + xyh_2^{16}h_3^{12} + h_2^{15}h_3^{45} + (y+1)h_2^{15}h_3^{30} + xyh_2^{15}h_3^{15} \\
& + (y+x)h_2^{15} + (x^2y+x^2)h_2^{14}h_3^{33} + (y+1)h_2^{14}h_3^{18} + h_2^{14}h_3^3 + yh_2^{13}h_3^{51} + xyh_2^{13}h_3^{36} \\
& + xh_2^{13}h_3^{21} + (xy+x)h_2^{13}h_3^6 + (y+x)h_2^{12}h_3^{54} + x^2yh_2^{12}h_3^{39} + (x^2y+x)h_2^{12}h_3^9 \\
& + (x^2y+x)h_2^{11}h_3^{42} + (y+x^2)h_2^{11}h_3^{27} + xh_2^{11}h_3^{12} + h_2^{10}h_3^{60} + (y+x^2)h_2^{10}h_3^{45} + xh_2^{10}h_3^{30} \\
& + (y+x)h_2^{10}h_3^{15} + (xy+1)h_2^{10} + (xy+x)h_2^9h_3^{63} + x^2yh_2^9h_3^{48} + (xy+x)h_2^9h_3^{33} \\
& + (xy+1)h_2^9h_3^{18} + (xy+x)h_2^9h_3^3 + xyh_2^8h_3^{51} + (x^2y+x)h_2^8h_3^{36} + (xy+x)h_2^8h_3^{21} \\
& + (y+x)h_2^8h_3^6 + (y+x)h_2^7h_3^{69} + (y+x^2)h_2^7h_3^{54} + (x^2y+1)h_2^7h_3^{39} + (xy+1)h_2^7h_3^{24} \\
& + xh_2^7h_3^9 + (xy+1)h_2^6h_3^{72} + xyh_2^6h_3^{42} + (xy+1)h_2^6h_3^{27} + (y+x^2)h_2^6h_3^{12} + xh_2^5h_3^{60} \\
& + (xy+1)h_2^5h_3^{45} + h_2^5h_3^{30} + (xy+x^2)h_2^5h_3^{15} + (y+1)h_2^5 + (xy+x)h_2^4h_3^{78} + yh_2^4h_3^{48} \\
& + (x^2y+x)h_2^4h_3^{33} + (xy+x)h_2^4h_3^{18} + x^2h_2^4h_3^3 + yh_2^3h_3^{81} + xyh_2^3h_3^{66} + xh_2^3h_3^{51} \\
& + (x^2y+x^2)h_2^3h_3^{36} + xyh_2^3h_3^{21} + (xy+x^2)h_2^2h_3^{69} + (y+x)h_2^2h_3^{54} + (y+1)h_2^2h_3^{39} \\
& + (y+x)h_2^2h_3^{24} + (y+x^2)h_2^2h_3^9 + (xy+1)h_2h_3^{87} + h_2h_3^{57} + x^2yh_2h_3^{42} + (x^2y+x^2)h_2h_3^{27} \\
& + (x^2y+1)h_2h_3^{12} + h_3^{90} + xh_3^{75} + h_3^{60} + x^2h_3^{45} + x^2h_3^{30} + 1.
\end{aligned}
$$

This equation does not describe the curve $X(1)$, since we did not consider isomorphism classes of A-Drinfeld modules yet. Therefore, let ψ be another A-Drinfeld module, with the same A-characteristic and normalized in the same way as ϕ, defined by

$$
\begin{aligned}
\psi_X &= l_0\tau^4 + l_1\tau^3 + l_2\tau^2 + l_3\tau + \iota(X), \\
\psi_Y &= t_0\tau^4 + t_1\tau^3 + t_2\tau^2 + t_3\tau + \iota(Y).
\end{aligned}
$$

An isomorphism between ϕ and ψ is a non-zero constant c such that $c\phi = \psi c$. By considering for example the leading coefficient of $c\phi_Y = \psi_Y c$ we get $c^{q^4-1} = 1$, implying that

$$
t_1^{(q+1)(q^2+1)} = h_1^{(q+1)(q^2+1)}; t_2^{q^2+1} = h_2^{q^2+1}; t_3^{(q+1)(q^2+1)} = h_3^{(q+1)(q^2+1)}. \tag{4.17}
$$

In other words, the quantities $h_1^{(q+1)(q^2+1)}$, $h_2^{q^2+1}$, $h_3^{(q+1)(q^2+1)}$ (and similarly $g_{11} := g_1^{(q+1)(q^2+1)}$, $g_{22} := g_2^{q^2+1}$, $g_{33} := g_3^{(q+1)(q^2+1)}$) are *invariants* of A-Drinfeld modules.

Putting $h_{22} := h_2^{q^2+1}$ and $h_{33} := h_3^{(q+1)(q^2+1)}$, the previously found equation $f(h_2, h_3) = 0$ relating h_2 and h_3, gives rise to a relation $p(h_{22}, h_{33}) = 0$. One simply uses the relations $f(h_2, h_3), h_2^{q^2+1} - h_{22}, h_3^{(q+1)(q^2+1)} - h_{33}$ and eliminates the variables h_2 and h_3 using a Groebner basis computation. The resulting relation $p(h_{22}, h_{33}) = 0$ then defines the Drinfeld modular curve $X(1)$. This is not immediately clear, since we strictly speaking only can be certain that the function field generated by h_{22} and h_{33} is a subfield of the function field of $X(1)$. However, again using a computer to perform a Groebner basis computation, one can show that this subfield already contains the remaining invariants $h_1^{(q+1)(q^2+1)}$, g_{11}, g_{22}, and g_{33}. At first sight it might look as if $\mathbb{F}_{16}(h_{22}, h_{33})$ has index 75 in $\mathbb{F}_{16}(h_2, h_3)$. With a computer it can be verified that h_2 can be expressed in h_{22} and h_3, implying that the index of $\mathbb{F}_{16}(h_{22}, h_{33})$ in $\mathbb{F}_{16}(h_2, h_3)$ in fact is only 15, in accordance with the number of possible choices of the isomorphism c mentioned before Equation (4.17).

So far, we have computed an explicit model for the curve $X(1)$. The theory implies that this curve has two components. Indeed, according to this prediction, the bivariate polynomial $p(t, s)$ is not absolutely irreducible, but has two absolutely irreducible factors, say $p^1(t, s)$ and $p^2(t, s)$, which turn out to have coefficients in $\mathbb{F}_{16}$. These factors define the curves that we previously denoted by $x^1(1)$ and $x^2(1)$.

To start a recursive description of a tower of function fields, we choose one of the components, say the one defined by $p^1(h_{22}, h_{33}) = 0$ defining the component denoted by $x^1(1)$. Since this curve has genus zero by Equation (4.8), its function field is rational and can be described using a parameter u, so $\mathbb{F}_{16}(h_{22}, h_{33}) = \mathbb{F}_{16}(u)$.

To describe a tower as in the previous section, we need to choose a prime ideal $\mathfrak{p}$. In this section we choose $\mathfrak{p} = \langle X, Y \rangle \subset A$, which is coprime with the A-characteristic $\langle X^2 + X + 1 \rangle$. Since $\deg \mathfrak{p} = 1$, a $\mathfrak{p}$-isogeny λ between ϕ and ψ is of the form $\tau - a$. From the isogeny property $\lambda\phi_Y = \psi_Y\lambda$ and using as before $x := \iota(X)$ and $y := \iota(Y)$, we get

$$t_3 = a^{-q}(y - y^q + ah_3), \tag{4.18}$$

$$t_2 = a^{-q^2}t_3 + a^{1-q^2}h_2 - a^{-q^2}h_3^q. \tag{4.19}$$

A direct verification shows that if we set $t_{33} = t_3^{(q+1)(q^2+1)}$ and $t_{22} = t_2^{q^2+1}$

then t_{33}, t_{22} satisfy $p^2(t_{22}, t_{33}) = 0$. In other words, the isogeny maps the component $x^1(1)$ of $X(1)$ to the other component $x^2(1)$. Similar to the uniformizing parameter u of $x^1(1)$, one can find a uniformizing parameter v of $x^2(1)$. Using the above isogeny relation, we can compute $\Phi^1(u, v) = 0$ defining $x_0^1(\mathfrak{p})$ like in Figure 4.4.

$$\begin{array}{ccc}
\mathbb{F}_{q^4}(u, h_2, h_3, a) & \overset{\lambda\phi=\psi\lambda}{=\!=\!=} & \mathbb{F}_{q^4}(v, t_2, t_3, a) \\
\Big| {\scriptstyle \lambda=\tau-a} & & \Big| \\
\mathbb{F}_{q^4}(u, h_2, h_3) & & \mathbb{F}_{q^4}(v, t_2, t_3) \\
{\scriptstyle h_{22}=h_2^{q^2+1}} \Big| {\scriptstyle h_{33}=h_3^{(q+1)(q^2+1)}} & & \Big| \\
\mathbb{F}_{q^4}(h_{22}, h_{33}) = \mathbb{F}_{q^4}(u) & & \mathbb{F}_{q^4}(v) = \mathbb{F}_{q^4}(t_{22}, t_{33})
\end{array}$$

Figure 4.4: Defining $x_0^1(\mathfrak{p})$ explicitly by $\Phi^1(u, v) = 0$.

Similarly, starting with the component $x^2(1)$, one finds the relation $\Phi^2(v, w) = 0$ defining $x_0^2(\mathfrak{p})$. Explicitly, one obtains:

$$\begin{aligned}
\Phi^1(u, v) &= (u + (x^2y + 1))v^3 \\
&\quad + (yu^3 + (xy + 1)u^2 + x^2yu + (xy + x))v^2 \\
&\quad + ((y + x^2)u^2 + (x^2y + 1)u + (xy + 1))v \\
&\quad + (y + 1)u^3 + xu^2 + yu + x^2y + x^2, \\
\Phi^2(v, w) &= (v + xy)w^3 \\
&\quad + ((y + x)v^3 + x^2yv^2 + xyv + 1)w^2 \\
&\quad + ((y + 1)v^2 + v + (y + 1))w \\
&\quad + (x^2y + x)v^3 + (y + x)v^2 + (xy + 1)v + xy.
\end{aligned}$$

Now we can construct the tower of function fields $\mathcal{F}/\mathbb{F}_{16} = (F_0, F_1, \cdots)$ corresponding to the modular tower $(x_0(\mathfrak{p}^k))_k$ by

1. $F_0 = \mathbb{F}_{16}(u_0)$,
2. $F_1 = F_0(u_1)$ with $\Phi^1(u_0, u_1) = 0$.
3. $F_k = F_{k-1}(u_k)$ where $\Phi^1(u_{k-1}, u_k) = 0$ if k odd, $\Phi^2(u_{k-1}, u_k) = 0$ otherwise.

As remarked in Section 4.4, for $k > 1$, the equations $\Phi^i(u_{k-1}, u_k) = 0$ give rise to two possible factors: one of degree one in u_k and one of degree $|\mathfrak{p}| = q = 2$. The factor of degree 2 should be chosen when defining the tower.

Acknowledgement

The authors would like to thank the anonymous referee for helpful suggestions and comments, that helped to improve the paper. The last two authors gratefully acknowledge the support from the Danish National Research Foundation and the National Science Foundation of China (Grant No.11061130539) for the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography as well as the support from The Danish Council for Independent Research (Grant No. DFF–4002-00367). The first author is supported by Tubitak Proj. No. 112T233.

Chapter 5

The exact limit of some cubic towers

Recently, a new explicit tower of function fields was introduced by Bassa, Beelen, Garcia and Stichtenoth (BBGS) [BBGS15]. This resulted in currently the best known lower bound for Ihara's constant in the case of non-prime finite fields. In particular over cubic finite fields, the tower's limit is at least as good as Zink's bound; i.e., $\lambda(\text{BBGS}/\mathbb{F}_{q^3}) \geq 2(q^2-1)/(q+2)$. In this chapter, the exact value of $\lambda(\text{BBGS}/\mathbb{F}_{q^3})$ is computed and the relationship between several towers is discussed. To do this, we examine one of the subtowers of Tower BBGS whose defining equation satisfies

$$\frac{(Y+1)^{N_n}}{Y^{N_j}} = \frac{(X+1)^{N_n}}{X^{q^{n-j}N_j}}\ , \tag{5.1}$$

where $N_i = (q^i-1)/(q-1)$ for $i \geq 1$ (see [BBGS15, Equation (38)]). We also settle a question stated by Ihara in [Iha07]. Apart from the introduction, the text of this chapter is as it was submitted in

[ABNed] N. Anbar, P. Beelen and N. Nguyen, The exact limit of some cubic towers, in *Arithmetic, geometry, cryptography and coding theory (AGCT 2015)*, submitted.

5.1 The subtower of Tower BBGS

In this section we investigate a subtower of Tower BBGS satisfying Equation (5.1) over cubic finite fields; i.e., $n = 3$. We denote $\mathbb{F}_{q^3}$ by $\mathbb{F}$.

5.1.1 The tower $\mathcal{Z}$

In the case of $j = 2$, Equation (5.1) becomes

$$\frac{(Y+1)^{q^2+q+1}}{Y^{q+1}} = \frac{(X+1)^{q^2+q+1}}{X^{q^2+q}} \ . \tag{5.2}$$

This equation is not irreducible. More precisely, the polynomial $(Y+1)^{q^2+q+1}X^{q^2+q} - Y^{q+1}(X+1)^{q^2+q+1}$ has two factors over $\mathbb{F}(X)$. One of them has degree $q+1$; namely

$$\begin{aligned} F(X,Y) &= X^{q+1}(Y+1)^{q+1} - (X+1)X^q(Y+1)^q - Y(X+1)^{q+1} \\ &= X^{q+1}Y^{q+1} - X^qY^q - X^qY - X^q - XY - Y, \end{aligned} \tag{5.3}$$

and the other factor has degree q^2. Later we will see that these two factors are absolutely irreducible (see the proof of Lemma 5.5). We are going to construct a tower $\mathcal{Z}/\mathbb{F} = (Z_i)_{i\geq 1}$ where $Z_i := \mathbb{F}(z_1, ..., z_i)$ and the recursion $F(z_i, z_{i+1}) = 0$ holds for F given in Equation (5.3) for each $i \geq 1$. Then $z_3 \in Z_3$ satisfies the polynomial equation

$$z_2^{q+1}(Y+1)^{q+1} - (z_2+1)z_2^q(Y+1)^q - Y(z_2+1)^{q+1} = 0 \ . \tag{5.4}$$

However, the left-hand side in Equation (5.4) is not irreducible over Z_2; in fact it has a factor of degree q given as follows.

$$(z_2Y - 1)\left(z_2Y + \frac{1}{z_1}\right)^{q-1} - \frac{(z_2+1)^q}{z_2} - \left(\frac{z_1+1}{z_1}\right)^q \tag{5.5}$$

Iteratively, Tower $\mathcal{Z}/\mathbb{F} = (Z_i)_{i\geq 1}$ is defined as a sequence of function fields satisfying $Z_2 = Z_1(z_2)$, where z_1, z_2 satisfy Equation (5.3); i.e.,

$F(z_1, z_2) = 0$ and $Z_{i+1} = Z_i(z_i)$ for $i \geq 2$, where

$$(z_i z_{i+1} - 1)\left(z_i z_{i+1} + \frac{1}{z_{i-1}}\right)^{q-1} - \frac{(z_i+1)^q}{z_i} - \left(\frac{z_{i-1}+1}{z_{i-1}}\right)^q = 0\ . \quad (5.6)$$

If we set $\alpha_0 := (z_1 z_2 - 1)/(z_1 + 1)$ then from $F(z_1, z_2) = 0$ in Equation (5.3) we get

$$z_1 = (\alpha_0 + 1)/\alpha_0^{q+1} \quad \text{and} \quad z_2 = \alpha_0^{q+1} + \alpha_0.$$

As a result, we see that $\mathbb{F}(\alpha_0) = \mathbb{F}(z_1, z_2) = Z_2$. Consider the tower $\mathcal{C}/\mathbb{F} = (C_i)_{i\geq 0}$ with $C_0 = \mathbb{F}(\alpha_0)$ and $C_{i+1} = C_i(\alpha_{i+1})$, where α_{i+1} satisfies the polynomial

$$T^{q+1} - \frac{1}{\alpha_i^{q+1} + \alpha_i} T - \frac{1}{\alpha_i^{q+1} + \alpha_i} \quad (5.7)$$

over $\mathbb{F}(\alpha_i)$ for all $i \geq 0$. In other words, $\frac{\alpha_{i+1}+1}{\alpha_{i+1}^{q+1}} = \alpha_i^{q+1} + \alpha_i$. Note that the polynomial (5.7) has a linear factor; namely $T + \frac{1}{\alpha_i+1}$; and hence for the construction of Tower $\mathcal{C}$ we consider the factor of degree q. We will see in Lemma 5.1 that for each $i \geq 0$ this factor is absolutely irreducible over C_i since there exists a place totally ramified in C_{i+1}/C_i lying over either $(\alpha_0 = 0)$ or $(\alpha_0 = \infty)$. This also implies the absolute irreducibility of the factor in (5.5) since Tower $\mathcal{C}$ is essentially the same as Tower $\mathcal{Z}$; i.e., $C_{i-2} = Z_i$ for $i \geq 2$ (see Figure 5.1).

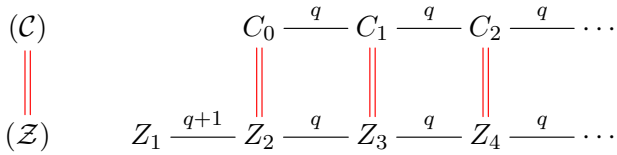

Figure 5.1: Tower $\mathcal{Z}/\mathbb{F}$ is the same of Tower $\mathcal{C}/\mathbb{F}$ as $C_{i-2} = Z_i$ for $i \geq 2$.

Moreover, Polynomial (5.7) defines the dual tower of Caro-Garcia [CG12] whose ramification was already clarified. With this information we state the ramification structure of Tower $\mathcal{C}$ as follows.

Lemma 5.1 (see [CG12])**.** *The ramification locus of Tower $\mathcal{C}$ contains exactly three places of C_0; namely $(\alpha_0 = -1)$, $(\alpha_0 = 0)$, and $(\alpha_0 = \infty)$. For a place Q of C_n, we set $P_i := Q \cap \mathbb{F}(\alpha_i)$ for $i = 0, \ldots, n$. Then the following holds.*

(i) If $P_i = (\alpha_i = -1)$ then $P_{i+1} = (\alpha_{i+1} = -1)$ or $P_{i+1} = (\alpha_{i+1} = \infty)$. In the first case, P_i is unramified in $\mathbb{F}(\alpha_i, \alpha_{i+1})/\mathbb{F}(\alpha_i)$ and P_{i+1} is totally ramified in $\mathbb{F}(\alpha_i, \alpha_{i+1})/\mathbb{F}(\alpha_{i+1})$ with different exponent q. However in the second case, both P_i and P_{i+1} ramified with ramification index $q-1$ in $\mathbb{F}(\alpha_i, \alpha_{i+1})/\mathbb{F}(\alpha_i)$ and $\mathbb{F}(\alpha_i, \alpha_{i+1})/\mathbb{F}(\alpha_{i+1})$, respectively.

(ii) If $P_i = (\alpha_i = 0)$ then $P_{i+1} = (\alpha_{i+1} = \infty)$. In this case, P_i is totally ramified in $\mathbb{F}(\alpha_i, \alpha_{i+1})/\mathbb{F}(\alpha_i)$ with different exponent q and P_{i+1} is unramified in $\mathbb{F}(\alpha_i, \alpha_{i+1})/\mathbb{F}(\alpha_{i+1})$.

(iii) If $P_i = (\alpha_i = \infty)$ then $P_{i+1} = (\alpha_{i+1} = 0)$. In this case, both P_i and P_{i+1} are unramified in $\mathbb{F}(\alpha_i, \alpha_{i+1})/\mathbb{F}(\alpha_i)$ and $\mathbb{F}(\alpha_i, \alpha_{i+1})/\mathbb{F}(\alpha_{i+1})$, respectively.

In particular, Figure 5.2 holds.

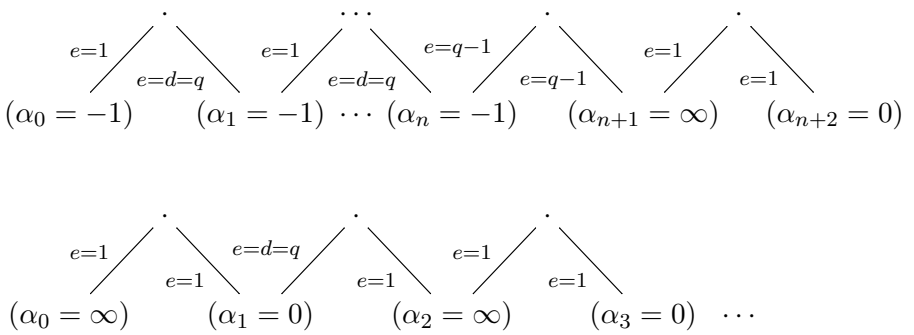

Figure 5.2: Ramification structure of Tower $\mathcal{C}/\mathbb{F}$.

In fact Tower $\mathcal{C}/\mathbb{F} = (C_i)_{i\geq 0}$ and Tower BeGS$/\mathbb{F} = (B_i)_{i\geq 1}$ of Bezerra, Garcia and Stichtenoth [BGS05b] are essentially the same. More precisely, it is shown in [CG12] that $C_i = B_i$ for all $i \geq 1$. Hence the exact genus of the function fields in Tower $\mathcal{C}$ can be given as follow (see [BGS05b]).

Proposition 5.2. *Let Tower $\mathcal{C} = (C_i)_{i\geq 0}$ defined as above. Then $g(C_i)$ is given as follows.*

1. *If* $i \equiv 0 \mod 4$ *then*

$$g(C_i) = \frac{1}{2(q-1)}\left(q^{i+1} + 2q^i - 2q^{\frac{i+2}{2}} - 2q^{i/2} + q\right) - \frac{i}{4}q^{\frac{i-2}{2}}(q+1) \ .$$

2. *If* $i \equiv 2 \mod 4$ *then*

$$g(C_i) = \frac{1}{2(q-1)}\left(q^{i+1} + 2q^i - 4q^{\frac{i+2}{2}} + q\right) - \frac{(i-2)}{4}q^{\frac{i-2}{2}}(q+1) \ .$$

3. *If* $i \equiv 1 \mod 2$ *then*

$$g(C_i) = \frac{1}{2(q-1)}\left(q^{i+1} + 2q^i - q^{\frac{i+3}{2}} - 3q^{\frac{i+1}{2}} + q\right) - \frac{(i-1)}{2}q^{\frac{i-1}{2}} \ .$$

Remark 5.3. In [Iha07] Ihara formulated a statement concerning the "basement" of Tower $\mathcal{Z}$. More precisely, he wrote that one could probably show that $\mathbb{F}(z_1) \cap \mathbb{F}(z_2) = \mathbb{F}$. However from Equation (5.2) we see that $\frac{(z_1+1)^{q^2+q+1}}{z_1^{q^2+q}} = \frac{(z_2+1)^{q^2+q+1}}{z_2^{q+1}}$, and hence $\frac{(z_1+1)^{q^2+q+1}}{z_1^{q^2+q}} \in \mathbb{F}(z_1) \cap \mathbb{F}(z_2)$.

For convenience we set $t_i := \frac{(z_i+1)^{q^2+q+1}}{z_i^{q^2+q}}$ for $i = 1, 2$. Then we have the following claim, which reveals the precise "basement" structure of Tower $\mathcal{Z}$.

Claim 1. *(i)* $\mathbb{F}(z_1) \cap \mathbb{F}(z_2) = \mathbb{F}\left(\frac{(z_1+1)^{q^2+q+1}}{z_1^{q^2+q}}\right)$.

(ii) Tower $\mathcal{Z}/\mathbb{F}$ *has no further sub-basement; i.e.,* $\mathbb{F}(t_1) \cap \mathbb{F}(t_2) = \mathbb{F}$.

Proof. To prove our claim we use the ramification structure of the places $(t_1 = \infty)$ and $(t_2 = \infty)$ in $\mathbb{F}(z_2)/\mathbb{F}(t_1)$ and $\mathbb{F}(z_2)/\mathbb{F}(t_2)$, respectively. One can show the following.

- $(z_2 = 0)$ and $(z_2 = \infty)$ are the only places of $\mathbb{F}(z_2)$ lying over $(t_1 = \infty)$ with $e((z_2 = 0)|(t_1 = \infty)) = q + 1$ and $e((z_2 = \infty)|(t_1 = \infty)) = d((z_2 = \infty)|(t_1 = \infty)) = q^2$.
- $(z_2 = 0)$ and $(z_2 = \infty)$ are the only places of $\mathbb{F}(z_2)$ lying over $(t_2 = \infty)$ with $e((z_2 = \infty)|(t_2 = \infty)) = 1$ and $e((z_2 = 0)|(t_2 = \infty)) = d((z_2 = 0)|(t_2 = \infty)) = q^2 + q$.

Suppose that $\mathbb{F}(v) := \mathbb{F}(z_1) \cap \mathbb{F}(z_2)$ properly contains $\mathbb{F}(t_1)$. As $q+1$ and q^2 are relatively prime, $(t_1 = \infty)$ can not ramify in $\mathbb{F}(v)/\mathbb{F}(t_1)$. That is, $(t_1 = \infty)$ has to split in $\mathbb{F}(v)$ since all two places of $\mathbb{F}(z_2)$ lying over $(t_1 = \infty)$ are rational. This shows that the extension degree $[\mathbb{F}(v) : \mathbb{F}(t_1)] = 2$. This gives a contradiction as 2 and q^2+q+1 are relatively prime. This proves item (i).

For the proof of item (ii), suppose that there exists an element $u \in \mathbb{F}(t_1) \cap \mathbb{F}(t_2)$ such that $\mathbb{F}(t_1)$ and $\mathbb{F}(t_2)$ are separable extensions of $\mathbb{F}(u)$. In this case, we consider the place $(z_2 = 0)$ of $\mathbb{F}(z_2)$. Note that $(z_2 = 0) \cap \mathbb{F}(u) = (u = \alpha)$ for some $\alpha \in \mathbb{F} \cup \{\infty\}$. In other words, we have

$$(z_2 = 0)|(t_1 = \infty)|(u = \alpha) \quad \text{and} \quad (z_2 = 0)|(t_2 = \infty)|(u = \alpha) \ .$$

Then by transitivity of ramification index and different exponent we obtain that

$$q^2 = (q+1)\left[d((t_1 = \infty)|(u = \alpha)) - qd((t_2 = \infty)|(u = \alpha))\right] \ .$$

This is a contradiction since the right hand side is a multiple of $q+1$, but the left hand side is not. □

5.1.2 The tower $\mathcal{G}$

In previous subsection, Tower $\mathcal{Z}$ was introduced, which is nothing else but the dual tower of Caro-Garcia in [CG12]. However, something new appears when we are trying to figure out the relation between the products $z_1 z_2$ and $z_3 z_4$.

Lemma 5.4. *The variables $z_1, ..., z_4$ in Tower $\mathcal{Z}$ satisfy*

$$\frac{(z_3 z_4 - 1)^{q^2+q+1}}{z_3 z_4} = \frac{(z_1 z_2 - 1)^{q^2+q+1}}{(z_1 z_2)^{q^2}} \ . \tag{5.8}$$

Proof. Note that z_3, z_4 also satisfy Equation (5.3); i.e.,

$$z_4(z_3+1)^{q+1} = z_3^{q+1}(z_4+1)^q(z_4+1) - (z_3+1)z_3^q(z_4+1)^q \ .$$

This holds if and only if

$$\frac{(z_3+1)^{q+1}}{z_3^q} = (z_4+1)^q \frac{(z_3z_4-1)}{z_4} \ . \tag{5.9}$$

On the other hand, expanding Equation (5.3) we get

$$(z_3z_4)^{q+1} - (z_3z_4)^q - z_3^q - z_3z_4 - z_3^q z_4 - z_4 = 0 \ . \tag{5.10}$$

Equation (5.10) shows that $(z_3z_4-1)^{q+1} = (z_3+1)^q(z_4+1)$. Then together with Equation (5.9) we obtain the following equalities.

$$\begin{aligned}\frac{(z_3z_4-1)^{q^2+q+1}}{z_3z_4} &= (z_3z_4-1)^{q^2+q}\frac{(z_3z_4-1)}{z_3z_4} \\ &= (z_3+1)^{q^2}(z_4+1)^q\frac{(z_3z_4-1)}{z_3z_4} \\ &= \frac{(z_3+1)^{q^2+q+1}}{z_3^{q+1}} \ .\end{aligned}$$

As the above relation also holds for z_1, z_2; i.e.,

$$\frac{(z_1z_2-1)^{q^2+q+1}}{z_1z_2} = \frac{(z_1+1)^{q^2+q+1}}{z_1^{q+1}} \ ,$$

together with Equation (5.2) we obtain the desired result as follows.

$$\begin{aligned}\frac{(z_1z_2-1)^{q^2+q+1}}{(z_1z_2)^{q^2}} = \frac{(z_1+1)^{q^2+q+1}}{z_1^{q^2+q}z_2^{q^2-1}} &= \frac{(z_2+1)^{q^2+q+1}}{z_2^{q^2+q}} \\ = \frac{(z_3+1)^{q^2+q+1}}{z_3^{q+1}} &= \frac{(z_3z_4-1)^{q^2+q+1}}{z_3z_4} \ .\end{aligned}$$

□

Now we define a subtower $\mathcal{G}/\mathbb{F} = (G_i)_{i\geq 1}$ of $\mathcal{Z}/\mathbb{F}$ by setting $G_i = \mathbb{F}(z_1z_2, ..., z_{2i-1}z_{2i})$ (see Figure 5.3).

From Lemma 5.4, we see that $\mathcal{G}/\mathbb{F}$ satisfies the recursive equation

$$\frac{(z_{2i-1}z_{2i}-1)^{q^2+q+1}}{(z_{2i-1}z_{2i})^{q^2}} = \frac{(z_{2i+1}z_{2i+2}-1)^{q^2+q+1}}{z_{2i+1}z_{2i+2}} \ .$$

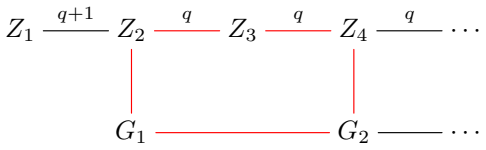

Figure 5.3: The subtower $\mathcal{G}/\mathbb{F}$ of $\mathcal{Z}/\mathbb{F}$.

Let $y_i = -1/z_{2i-1}z_{2i}$ for $i = 1, 2$. From Equation (5.8) we see that

$$\frac{(y_1+1)^{q^2+q+1}}{y_1^{q+1}} = \frac{(y_2+1)^{q^2+q+1}}{y_2^{q^2+q}} \ . \tag{5.11}$$

As mentioned before, Equation (5.11) has two factors, one of degree $q+1$, the other of degree q^2. We will show that Tower $\mathcal{G}$ is recursively defined by the degree-q^2 factor of Equation (5.11). In order to prove that $[G_2 : G_1] = q^2$, we will show that $[Z_2 : G_1] = [Z_4 : G_2] = q+1$.

Lemma 5.5. *Let $\mathcal{G}/\mathbb{F} = (G_i)_{i\geq 1}$ be the subtower of $\mathcal{Z}/\mathbb{F} = (Z_i)_{i\geq 1}$ defined as above. Then the following holds.*

(i) $Z_2 = G_1(z_2)$ *and* $[Z_2 : G_1] = q+1$.

(ii) $Z_4 = G_2(z_2)$.

(iii) $[Z_4 : G_2] = q+1$ *and* $[G_2 : G_1] = q^2$.
See Figure 5.4.

Proof. It is clear that $Z_2 = \mathbb{F}(z_1, z_2) = \mathbb{F}(z_1z_2, z_2) = G_1(z_2)$. Multiplying $F(z_1, z_2)$ by z_2^q, we see that z_2 satisfies the following polynomial over $\mathbb{F}(z_1z_2)$.

$$T^{q+1} - \left((z_1z_2)^{q+1} - (z_1z_2)^q - z_1z_2\right)T^q + (z_1z_2)^qT + (z_1z_2)^q \ , \tag{5.12}$$

where F is the polynomial given in Equation (5.3). In other words, z_2 satisfies a polynomial over G_1 of degree $q+1$. This shows that $[Z_2 : G_1] \leq q+1$. Now replacing T in Equation (5.12) by z_1z_2T and then dividing by $(z_1z_2)^{q+1}$ we obtain the following polynomial.

$$T^{q+1} - \left((z_1z_2)^q - (z_1z_2)^{q-1} - 1\right)T^q + T + \frac{1}{z_1z_2} \tag{5.13}$$

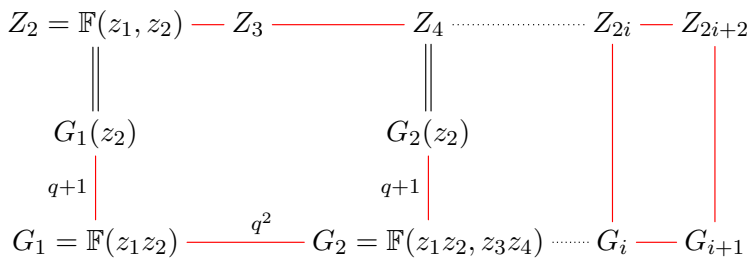

Figure 5.4: Relationship between towers $\mathcal{Z}/\mathbb{F}$ and $\mathcal{G}/\mathbb{F}$.

We see from Equation (5.13) that the place ($z_1 z_2 = 0$) of G_1 satisfies Eisenstein's Irreducibility Criterion ([Sti09, Proposition 3.1.15]). This shows that the extension degree is equal to $q + 1$, which gives the proof of (i).

In order to prove that $G_2(z_2) = Z_4$, it is enough to show that $z_3 \in G_2(z_2)$ (since then $z_4 = z_3 z_4 / z_3$ also belongs to $G_2(z_2)$). From Equation (5.6) we get $u := (z_3 + 1)^q / z_3 \in \mathbb{F}(z_3 z_4, z_2)$. Then dividing Equation (5.4) by z_3 and using the fact that $u \in \mathbb{F}(z_3 z_4, z_2)$, we get $v := (z_3 + 1)^{q+1} / z_3$ also lies in $\mathbb{F}(z_3 z_4, z_2)$. As a result, the element $z_3 + 1 = v/u \in \mathbb{F}(z_3 z_4, z_2) \subset G_2(z_2)$ and this finishes the proof of (ii).

Since $G_2 = G_1(z_3 z_4)$ and $[G_1(z_2) : G_1] = q + 1$, we have $[Z_4 : G_2] = [G_2(z_2) : G_2] \leq q + 1$. Furthermore, we have $[G_2 : G_1] \leq q^2$ since Equation (5.11) has two factors of degree $q + 1$ and q^2. Then from the facts that $[Z_2 : G_1] = q+1$ and $[Z_4 : Z_2] = q^2$, we obtain $[Z_4 : G_2] = q+1$ and $[G_2 : G_1] = q^2$. □

The proof of Lemma 5.5 still works recursively along the two towers $\mathcal{Z}/\mathbb{F}$ and $\mathcal{G}/\mathbb{F}$. In other words we see that $Z_{2i} = G_i(z_2)$, and the total ramification of the place ($z_1 z_2 = 0$) in Z_2/G_1 implies that the extension degree is $[Z_{2i} : G_i] = q + 1$. In summary, we have the following relation between Tower $\mathcal{Z}$ and Tower $\mathcal{G}$.

Corollary 5.6. *For all $i \geq 1$, we have*

(i) $Z_{2i} = G_i(z_2)$ *and* $[Z_{2i} : G_i] = q + 1$.

(ii) $[G_{i+1} : G_i] = q^2$.

For $i = 1$, *item (ii) also follows from [BBGS15], but for* $i \geq 1$ *it is new.*

Remark 5.7. The existence of rational places of G_{i+1} for each $i \geq 1$ shows that the degree-q^2 factor of Equation (5.11) is absolutely irreducible over G_i.

5.2 The exact genus and exact limit of Tower $\mathcal{G}$

The ramification structure of Tower $\mathcal{G}$ can be clarified like the ramification structure of Tower $\mathcal{Z}$. In this section, for each $i \geq 1$ we compute the exact value of the genus $g(G_i)$. After that the exact limit of the tower is determined. In this section we denote by $\mathbb{F}$ the algebraic closure of $\mathbb{F}_{q^3}$.

5.2.1 Exact genus $g(G_i)$

Given the exact value of $g(Z_{2i})$, the exact value of $g(G_i)$ for each $i \geq 1$ can be computed using the Hurwitz genus formula once we know the ramification and different in the extension Z_{2i}/G_i. Looking at the field extensions

$$G_i \subseteq G_{i+1} \subseteq Z_{2i+2} \quad \text{and} \quad G_i \subseteq Z_{2i} \subseteq Z_{2i+2}$$

for $i \geq 1$ (see Figure 5.4), the ramification of Z_{2i+2}/G_{i+1} can be determined recursively by studying the ramification in Z_{2i}/G_i and G_{i+1}/G_i. For this reason, we first determine the ramification in Z_2/G_1.

Lemma 5.8. *Let* $G_1 = \mathbb{F}(z_1 z_2)$ *and* $Z_2 = G_1(z_2)$. *Then the ramification in* Z_2/G_1 *can be given as follows.*

(i) The place $(z_1 z_2 = 0)$ *is totally ramified; i.e., the ramification index is* $q + 1$.

(ii) *There are exactly two places P_1, P_2 of Z_2 lying above $P_\infty := (z_1 z_2 = \infty)$ with $e(P_1|P_\infty) = d(P_1|P_\infty) = q$ and $e(P_2|P_\infty) = 1$.*

(iii) *$(z_1 z_2 = 0)$ and $(z_1 z_2 = \infty)$ are the only ramified places of G_1.*

Proof. From the proof of Lemma 5.5 item (i), we see that the place $(z_1 z_2 = 0)$ is totally ramified with ramification index $q + 1$.

For the proof of item (ii), we set $z := 1/z_1 z_2$ so that $(z_1 z_2 = \infty)$ becomes the place $(z = 0)$. Then by replacing T in (5.13) by T/z^q and then multiplying by z^{q^2+q} we obtain

$$p(T) = T^{q+1} - (z^q + z - 1)T^q + Tz^{q^2} + z^{q^2+q+1} \ . \tag{5.14}$$

Let y be a root of $p(T)$. Then $Z_2 = \mathbb{F}(z, y)$ and by Kummer's Theorem (see [Sti09, Theorem 3.3.7]), we conclude that there exist places P_1 and P_2 of Z_2 lying over $(z = 0)$ such that

$$z, y \in P_1 \quad \text{and} \quad z, y + 1 \in P_2 \ .$$

Now we show that the ramification index $e(P_1|(z = 0)) = q$. As a result, we conclude that P_1 and P_2 are the only places lying over $(z = 0)$ and $e(P_2|(z = 0)) = 1$. First of all, by the Fundamental Equality (see [Sti09, Theorem 3.1.11]) we note that $e(P_1|(z = 0)) \leq q$. We consider

$$p(y) = y^q(y - (z^q + z - 1)) + yz^{q^2} + z^{q^2+q+1} = 0 \ ,$$

or equivalently

$$\left(\frac{y}{z^{q+1}}\right)^q (y - z^q - z + 1) = -z\left(\frac{y}{z^{q+1}} + 1\right).$$

By the Strict Triangle Inequality, we see that $v_{P_1}\left(\frac{y}{z^{q+1}}\right) > 0$, further implying that $q \cdot v_{P_1}\left(\frac{y}{z^{q+1}}\right) = v_{P_1}(z) > 0$. This shows that $e(P_1|(z = 0)) = v_{P_1}(z)$ is a positive multiple of q.

Let $P = (z = \alpha)$ for some $\alpha \in \mathbb{F} \setminus \{0\}$, where $z = 1/z_1 z_2$ as above. We consider the minimal polynomial $p(T)$ of y over $\mathbb{F}(z)$ (see Equation (5.14)) and denote by $p_\alpha(T)$ the polynomial given by

$$p_\alpha(T) = T^{q+1} - (z(P)^q + z(P) - 1)T^q + Tz(P)^{q^2} + z(P)^{q^2+q+1} \ ,$$

where $z(P) = \alpha$ is the evaluation of the function z at P. Note that $p_\alpha(T)$ has a multiple root in $\mathbb{F}$ if and only if $\alpha = 0$ or $\alpha = 1$. As a result, we conclude that each place $P = (z = \alpha)$ for $\alpha \in \mathbb{F} \setminus \{0, 1\}$ is unramified in Z_2/G_1. To finish the proof of item (iii), we show that $(z = 1)$ is not ramified either. For this we replace T by $T-1$ in Equation (5.14) so that $y + 1$ is a root of

$$T^{q+1} - (z-1)^{q+1}T^q + (z-1)^q T + (z-1)^{q+1} \ .$$

Then we replace T by $-(z-1)T$ and then divide by $(z-1)^{q+1}$; and hence we obtain the polynomial

$$T^{q+1} + (z-1)^q T^q - T + 1 \ .$$

Note that $T^{q+1} - T + 1$ is a separable polynomial. Therefore Kummer's Theorem implies that there is no ramification over the place $(z = 1)$. This finishes the proof of (iii).

To finish the proof of item (ii), we conclude by the Hurwitz genus formula that the different exponent is $d(P_1|P_\infty) = q$ since $Z_2 = C_0$ is a rational function field. □

Now we state the ramification structure of the subtower $\mathcal{G}/\mathbb{F}_{q^3}$. For convenience we first fix some notation. Let Q be a place of $G_n = \mathbb{F}(z_1 z_2, \ldots, z_{2n-1} z_{2n})$ for some $n \geq 1$. We denote by P_i the restriction of Q to $\mathbb{F}(z_{2i-1} z_{2i})$; i.e., $P_i = Q \cap \mathbb{F}(z_{2i-1} z_{2i})$ for all $i = 1, \ldots, n$.

Lemma 5.9. *Let $\mathcal{G}/\mathbb{F} = (G_i)_{i \geq 1}$ be the tower given as before. The ramification locus of Tower $\mathcal{G}$ consists of exactly two places of G_1; namely $(z_1 z_2 = 0)$ and $(z_1 z_2 = \infty)$. Denoted by $\zeta_i = z_{2i-1} z_{2i}$ for $i \geq 1$, the following holds.*

(i) If $P_i = (\zeta_i = 0)$ then $P_{i+1} = (\zeta_{i+1} = 0)$ or $P_{i+1} = (\zeta_{i+1} = \infty)$. In the first case, P_i is unramified in $\mathbb{F}(\zeta_i, \zeta_{i+1})/\mathbb{F}(\zeta_i)$ and P_{i+1} is totally ramified in $\mathbb{F}(\zeta_i, \zeta_{i+1})/\mathbb{F}(\zeta_{i+1})$ with different exponent q^2. In the second case, P_i is ramified in $\mathbb{F}(\zeta_i, \zeta_{i+1})/\mathbb{F}(\zeta_i)$ with ramification index $q^2 - 1$, and P_{i+1} is ramified in $\mathbb{F}(\zeta_i, \zeta_{i+1})/\mathbb{F}(\zeta_{i+1})$ with ramification index $q^2 - q$ and different exponent $q^2 - 2$.

(ii) If $P_i = (\zeta_i = \infty)$ then $P_{i+1} = (\zeta_{i+1} = \infty)$. In this case, P_i is ramified in $\mathbb{F}(\zeta_i, \zeta_{i+1})/\mathbb{F}(\zeta_i)$ with ramification index and different exponent q, and P_{i+1} is unramified in $\mathbb{F}(\zeta_i, \zeta_{i+1})/\mathbb{F}(\zeta_{i+1})$.

In particular, Figure 5.5 holds.

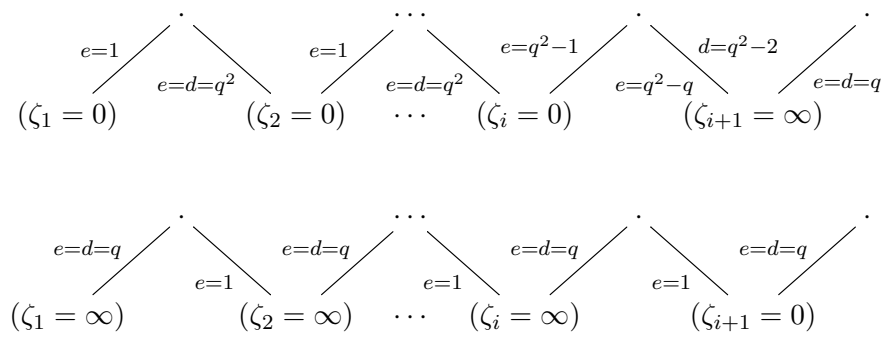

Figure 5.5: Ramification structure of Tower $\mathcal{G}/\mathbb{F}$.

Proof. Let $y_i = -1/\zeta_i$ for $i = 1, 2$, then y_1, y_2 satisfy Equation (5.11) defining the dual tower of a tower whose ramification was explored in [BBGS15]. The ramification of Tower $\mathcal{Z}$ was depicted in Figures 2, 3, 4 in [BBGS15], and we read the ramification from right to left. □

Theorem 5.10. *Let $\mathcal{G}/\mathbb{F} = (G_i)_{i\geq 1}$ be the tower given as before. The genus $g(G_i)$ of the function field G_i is given as follow.*

(i) If $i \geq 1$ is odd

$$\begin{aligned} g(G_i) =& \frac{1}{2(q+1)}[\frac{1}{q-1}(q^{2i-1} + 2q^{2i-2} - 2q^i - 2q^{i-1} + q) \\ & - (i-1)q^{i-2}(q+1) - 2 - q(q^{i-1}+1)] + 1 \ . \end{aligned}$$

(ii) If $i > 1$ is even

$$\begin{aligned} g(G_i) =& \frac{1}{2(q+1)}[\frac{1}{q-1}(q^{2i-1} + 2q^{2i-2} - 4q^i + q) \\ & - (i-2)q^{i-2}(q+1) - 2 - q(q^{i-1}+1)] + 1 \ . \end{aligned}$$

Proof. Instead of Tower $\mathcal{Z}$, we work with Tower $\mathcal{C}$ using the relation $C_{i-2} = Z_i$. Consider the field extension C_{2i-2}/G_i for $i \geq 1$ and compute the genus of G_i based on $g(C_{2i-2})$. First note that $z_1 z_2 = (1+\alpha_0)^{q+1}/\alpha_0^q$. As a result, we deduce that

$$z_1 z_2 = 0 \text{ if and only if } \alpha_0 = -1 \ ,$$

and

$$z_1 z_2 = \infty \text{ if and only if } \alpha_0 = 0 \text{ or } \alpha_0 = \infty \ .$$

Then by Lemmas 5.1 and 5.8, we conclude that a place Q of C_{2i-2} is ramified in C_{2i-2}/G_i only if $Q \cap \mathbb{F}(\alpha_0)$ is $(\alpha_0 = 0)$ or $(\alpha_0 = -1)$. Hence we investigate the ramification in these two cases.

(i) $\underline{Q \cap \mathbb{F}(\alpha_0) = (\alpha_0 = 0)}$:

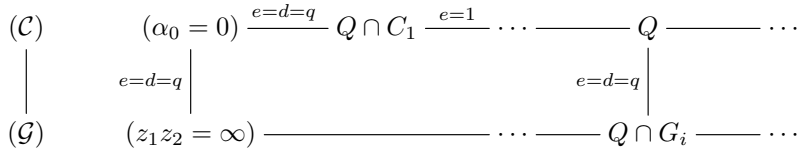

Figure 5.6: Case 1: Starting from $(\alpha_0 = 0)$ in C_0.

From Lemmas 5.1 and 5.9, for each place Q in C_{2i-2} lying over $(\alpha_0 = 0)$, we have

$$e(Q|(\alpha_0 = 0)) = e((Q \cap G_i)|(z_1 z_2 = \infty)) = q^{i-1} \text{ and}$$
$$d(Q|(\alpha_0 = 0)) = d((Q \cap G_i)|(z_1 z_2 = \infty)) = q\frac{q^{i-1}-1}{q-1} \ .$$

By transitivity of the different we conclude that Q is ramified in C_{2i-2}/G_i with

$$e(Q|(Q \cap G_i)) = d(Q|(Q \cap G_i)) = q \ ,$$

for $i \geq 1$. Since the place $(\alpha_0 = 0)$ is totally ramified and splits completely in an alternating way in Tower $\mathcal{C}$, the number of places of C_{2i-2} lying over $(\alpha_0 = 0)$ is q^{i-1}.

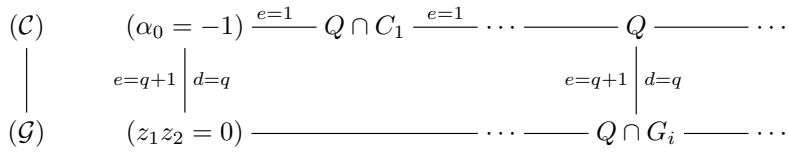

Figure 5.7: Case 2: Starting from $(\alpha_0 = -1)$ in C_0.

(ii) $Q \cap \mathbb{F}(\alpha_0) = (\alpha_0 = -1)$:
A place Q of C_{2i-2} lying over $(\alpha_0 = -1)$ contributes to the ramification of C_{2i-2}/G_i for $i \geq 1$ if and only if $\alpha_0(Q) = \alpha_1(Q) = \cdots = \alpha_{2i-2}(Q) = -1$. However, from Lemma 5.1 there is a unique place Q with this property.

Using the Hurwitz genus formula and the exact genus of each C_{2i-2} formulated in Proposition 5.2 we get the exact genus $g(G_i)$ of G_i for each $i \geq 1$. □

5.2.2 Exact limit

The exact limit of a tower can be computed if we know the exact genus and the exact number of rational places of every function field along the tower like the tower in [vdGvdV02]. However in general it is not easy to compute these exact values. Here we apply the procedures in [BGS05a] based on the results in [Bee04] to compute the exact limit $\lambda(\mathcal{G})$. In order to apply that approach we have to transform the defining equation of Tower $\mathcal{G}$ into a special form of polynomial, called type A.

A polynomial $f(X, Y) \in \mathbb{F}_q[X, Y]$ is called a *polynomial of type* A if $f(X, Y) = \varphi(Y)\psi_1(X) - \psi_0(X)$ for some polynomials $\varphi(Y) \in \mathbb{F}_q[Y]$ and $\psi_0(X), \psi_1(X) \in \mathbb{F}_q[X]$ such that $\varphi(Y)$ and $\psi_0(X)$ are monic and of the same degree with $0 < \deg \psi_0 - \deg \psi_1 < \deg \varphi$. A tower recursively defined by polynomial of type A is called a *tower of type A*.

We note that $G_2 = \mathbb{F}_{q^3}(z_1z_2, z_3z_4)$ is rational by Theorem 5.10. Therefore, we can find a uniformizer element $a \in G_2$ such that z_1z_2 and z_3z_4

can be expressed as rational functions in a. Such a uniformizer element a and rational functions can be computed as follows.

Lemma 5.11. *There exists an element $a \in G_2 = \mathbb{F}_{q^3}(z_1z_2, z_3z_4)$ such that z_1z_2 and z_3z_4 can be expressed as rational functions in a.*

Proof. Let $y_1 = -1/z_1z_2$, $y_2 = -1/z_3z_4$, then $G_2 = \mathbb{F}_{q^3}(y_1, y_2)$ where y_1, y_2 satisfy Equation (5.11). We set

$$t_1 := \frac{y_2+1}{y_2(y_1+1)} \quad \text{and} \quad t_2 := \frac{1}{y_1} \ .$$

Then $\mathbb{F}_{q^3}(t_1, t_2) = \mathbb{F}_{q^3}(y_1, y_2) = G_2$ and Equation (5.11) implies that

$$\begin{aligned} t_1^{q^2+q+1} = \frac{1}{y_2 y_1^{q+1}} &= \frac{y_2+1}{y_2(y_1+1)}\left(\frac{1}{y_1^{q+1}} + \frac{1}{y_1^q}\right) - \frac{1}{y_1^{q+1}} \\ &= t_1(t_2^{q+1} + t_2^q) - t_2^{q+1} \ , \end{aligned}$$

which has two irreducible factors mentioned in previous section. More precisely, if we set $\tilde{F} := t_1^{q+1} + t_1t_2 - t_2$, then

$$t_1^{q^2+q+1} - t_1(t_2^{q+1} + t_2^q) + t_2^{q+1} = \tilde{F}(t_1\tilde{F}^{q-1} - t_2^q) = 0 \ ,$$

and G_2 is defined by the factor $t_1\tilde{F}^{q-1} - t_2^q = 0$, which implies that

$$\frac{\tilde{F}^{q-1}}{t_2^{q-1}} = \frac{t_2}{t_1} \ . \tag{5.15}$$

We set $a := \frac{\tilde{F}}{t_1t_2}$. Then from the definition of $\tilde{F}$ and Equation (5.15) we get the following equivalent equations.

$$\begin{aligned} \frac{\tilde{F}}{t_2} &= \frac{t_2^{q-1}}{\tilde{F}^{q-1}} t_1^q + t_1 - 1 \\ 1 &= \frac{t_2^q}{\tilde{F}^q} t_1^q + \frac{t_1t_2}{\tilde{F}} - \frac{t_2}{\tilde{F}} \\ \frac{t_2}{\tilde{F}} &= \frac{1}{a^q} + \frac{1}{a} - 1 \end{aligned}$$

In other words, from the definition of a, we have

$$\frac{1}{t_1} = \frac{t_2 a}{\tilde{F}} = a^{1-q} + 1 - a$$

and

$$\frac{1}{t_2} = \frac{at_1}{\tilde{F}} = a\frac{t_2^q}{\tilde{F}^q} = a^{1-q^2} + a^{1-q} - a \ .$$

Then by using the definitions of t_1 and t_2 we get

$$z_1 z_2 = -\frac{1}{y_1} = -t_2 = \frac{-a^{q^2-1}}{1 + a^{q^2-q} - a^{q^2}}$$

and

$$z_3 z_4 = -\frac{1}{y_2} = 1 - t_1(y_1 + 1) = \frac{-1}{a^{q^2-q} + a^{q^2-1} - a^{q^2}} \ .$$

□

As a result, Tower $\mathcal{G}$ starting with G_2 can be recursively defined by a new equation

$$\frac{-a_2^{q^2-1}}{1 + a_2^{q^2-q} - a_2^{q^2}} = \frac{-1}{a_1^{q^2-q} + a_1^{q^2-1} - a_1^{q^2}} \ ,$$

or

$$\frac{a_2^{q^2} - a_2^{q^2-q} - 1}{a_2^{q^2-1}} = a_1^{q^2} - a_1^{q^2-1} - a_1^{q^2-q} \ , \tag{5.16}$$

which is the dual of a tower of type A.

Theorem 5.12. *Let $\mathcal{G} = (G_1 \subset G_2 \subset \cdots)$ be the tower given as before. Then*

$$\lambda(\mathcal{G}/\mathbb{F}_{q^3}) = 2(q^2 - 1)/(q + 2) \ .$$

Proof. Since G_2 is rational, Tower $\mathcal{G}$ can be started with G_2 and recursively defined by equation (5.16). Each $\alpha \in \overline{\mathbb{F}}_{q^3}$ satisfying the equation

$$\alpha^{q^2} - \alpha^{q^2-1} - \alpha^{q^2-q} - 1 = 0$$

lies in $\mathbb{F}_{q^3}$. Hence from Equation (5.16) we can see that such a value of $\alpha \in \mathbb{F}_{q^3}$ describes a place in G_2 splitting completely in the tower $\mathcal{G}$. We observe from Theorem 5.10 (see Figure 5.6) that G_i has q^i places lying over $(z_1 z_2 = \infty)$. Furthermore, the number of places of G_i lying over $(z_1 z_2 = 0)$ is the same as the number of places of C_{2i-2} lying over

($\alpha_0 = -1$) (see Figure 5.7) which lies in $O\left(q^{i-1}\right)$ by Propositions 2.7 and 2.8 in [BGS05b]. As a result, we see that the places of G_i for $i > 1$ lying above the ramification locus of $\mathcal{G}$ do not contribute asymptotically to the splitting rate of $\mathcal{G}$ over G_2, which is defined by

$$\nu(\mathcal{G}/G_2) := \lim_{i\to\infty} \frac{N(G_i)}{[G_i : G_2]} .$$

Applying results in [Bee04] we have $\nu(\mathcal{G}/G_2)$ equals the cardinality of the splitting locus of $\mathcal{G}$ over G_2, which is defined by

$$t(\mathcal{G}/G_2) := \#\{P \text{ a rational place of } G_2 \mid P \text{ splits completly in } \mathcal{G}\}.$$

Moreover, from Theorem 5.10 we get that the genus of Tower $\mathcal{G}$ over G_2 equals

$$\gamma(\mathcal{G}/G_2) := \lim_{i\to\infty} \frac{g(G_i)}{[G_i : G_2]} = \frac{q^2(q+2)}{2(q^2-1)} .$$

Since $\mathcal{G}/\mathbb{F}_{q^3}$ is a dual tower of a tower of type A, the same argument in [BGS05a, Example 5.5.] (when dealing with Tower BeGS) can be applied to Tower $\mathcal{G}$. More precisely, we have $\nu(\mathcal{G}/G_2) = t(\mathcal{G}/G_2) = q^2$ and

$$\lambda(\mathcal{G}/\mathbb{F}_{q^3}) = \frac{\nu(\mathcal{G}/G_2)}{\gamma(\mathcal{G}/G_2)} = \frac{2(q^2-1)}{(q+2)} .$$

□

Corollary 5.13. *The exact limit* $\lambda(\mathrm{BBGS}/\mathbb{F}_{q^3})$ *of Bassa, Beelen, Garcia and Stichtenoth tower over cubic finite fields equals to*

$$\lambda(\mathrm{BBGS}/\mathbb{F}_{q^3}) = \frac{2(q^2-1)}{(q+2)} .$$

Proof. The inequality $\lambda(\mathrm{BBGS}/\mathbb{F}_{q^3}) \geq 2(q^2-1)/(q+2)$ is shown in [BBGS15]. On the other hand, $\lambda(\mathrm{BBGS}/\mathbb{F}_{q^3}) \leq 2(q^2-1)/(q+2)$ follows from the fact that $\mathcal{G}/\mathbb{F}_{q^3}$ is a subtower of $\mathrm{BBGS}/\mathbb{F}_{q^3}$. □

5.3 Conclusion

Tower $\mathcal{G}$ introduced in [BBGS15] is related to previously studied towers over cubic finite fields $\mathbb{F}_{q^3}$ (see Figure 5.8). This relation is used to show

that the exact limit of Tower $\mathcal{G}$ is equal to $2(q^2-1)/(q+2)$. As a consequence, also tower BBGS/$\mathbb{F}_{q^3}$ has this limit.

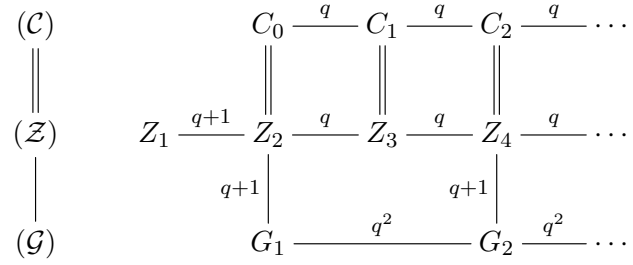

Figure 5.8: Relations between the towers.

Acknowledgment

Nurdagül Anbar and Peter Beelen gratefully acknowledge the support from The Danish Council for Independent Research (Grant No. DFF–4002-00367). Nurdagül Anbar is also supported by a H.C. Ørsted COFUND Post-doc Fellowship from the project "Algebraic curves with many rational points".

Chapter 6

Further developments and future work

The first two sections of this chapter discuss some further developments related to the article in Chapter 4. The discussion in the last two sections is for future work.

6.1 Another optimal tower over $\mathbb{F}_{16}$

In Section 4.5, we successfully constructed an optimal tower $\mathcal{F}/\mathbb{F}_{2^8}$ of Drinfeld modular curves as an example of Theorem 4.5 when $A \neq \mathbb{F}_q[T]$. In this section, we introduce another example of an optimal tower over $\mathbb{F}_{16}$ that is still not fully explained with Drinfeld modular theory. This tower was actually found[1] before we could fully prove the theory in Chapter 4; i.e., at that time we still did not know how to choose the parameters to get optimal towers of Drinfeld modular curves.

[1]The tower was found and was presented at Sabancı Üniversitesi, İstanbul during the Ph.D. external research in the winter of 2013-2014 under the support of Otto Mønsted Fond.

We use the same setting and the same construction in Section 4.5 but with another A-characteristic P. More precisely, we consider the following setting:

(i) $F/\mathbb{F}_q := \mathbb{F}_2(X,Y)/\mathbb{F}_2$, where $Y^2 + XY + X^2 = X$ and X is transcendental over $\mathbb{F}_2$.

(ii) $A := \mathbb{F}_2[X,Y]$, implying $\delta = 2$.

(iii) The A-characteristic P is the ideal $\langle X, Y\rangle \subset A$.

In this case, $d = \deg P = 1$, $e = \operatorname{ord} P = 2$ and $\iota(X) = \iota(Y) = 0$. We consider the rank 2 Drinfeld A-module ϕ specified by

$$\phi_X = g_0\tau^4 + g_1\tau^3 + g_2\tau^2 + g_3\tau,$$
$$\phi_Y = h_0\tau^4 + h_1\tau^3 + h_2\tau^2 + h_3\tau.$$

The Drinfeld module ϕ is also normalized by putting $h_0 = 1$ and $g_0 \in \mathbb{F}_4$ such that $g_0^2 + g_0 + 1 = 0$. We chose $\mathfrak{p} = \langle X - 1, Y\rangle \subset A$ coprime with P for $\mathfrak{p}$-isogeny of degree one $\lambda = \tau - a$.

Assume that α is a primitive element of $\mathbb{F}_4$. Following the same construction in Section 4.5 we obtain the tower $\mathcal{G} = (G_0, G_1, ...)$ defined over $\mathbb{F}_4$ corresponding to Drinfeld modular curves $(x_0(\mathfrak{p}^i))_{i\geq 0}$ where $G_0 = \mathbb{F}_4(u_0)$, $G_1 = G_0(u_1)$ with

$$u_1^3 + (u_0+1)u_1^2 + (\alpha^2u_0^2 + \alpha u_0 + \alpha)u_1 + \alpha^2u_0^3 + u_0 + \alpha^2 = 0,$$

and $G_{i+1} = G_i(u_{i+1})$ with

$$\Psi(u_{i-1}, u_i, u_{i+1}) = 0,$$

where Ψ is the factor of degree two of

$$u_{i+1}^3 + (u_i+1)u_{i+1}^2 + (\alpha_i^2u_i^2 + \alpha_iu_i + \alpha_i)u_{i+1} + \alpha_i^2u_i^3 + u_i + \alpha_i^2, \quad (6.1)$$

and $\alpha_i = \alpha^{2^i}$ for $i \geq 1$. For having many rational places, we consider the tower over $\mathbb{F}_{16} = \mathbb{F}_{q^{2de}}$. We compute the limit of the tower by exploring the ramification structure and the splitting structure to conclude that $\lambda(\mathcal{G}/\mathbb{F}_{16}) \geq 1$.

Noticing that $G_1 = \mathbb{F}_4(u_0, u_1)$ is rational (by computing the genus $g(G_1) = 0$), there exists uniformizers $v_0 \in \mathbb{F}_4(u_0, u_1)$ and $v_1 \in \mathbb{F}_4(u_1, u_2)$ such that u_1 can be expressed as rational functions in v_0 and v_1. Assume that $u_1 = \varphi_0(v_0)/\varphi_1(v_0) \in \mathbb{F}_4(v_0)$ and $u_1 = \psi_0(v_1)/\psi_1(v_1) \in \mathbb{F}_4(v_1)$ for some polynomials $\varphi_i(v_0) \in \mathbb{F}_4[v_0], \psi_i \in \mathbb{F}_4[v_1]$. Finding such polynomials can be done using Magma for example. In particular, the polynomial

$$\psi_0(v_1)\varphi_1(v_0) - \varphi_0(v_0)\psi_1(v_1)$$

has the following factor

$$\begin{aligned} f(v_0, v_1) &:= v_0^2 v_1^2 + \alpha v_0^2 v_1 + \alpha v_0^2 + \alpha v_0 v_1^2 + \alpha^2 v_0 v_1 + v_1^2 + v_1 \\ &= (v_0^2 + \alpha v_0 + 1)v_1^2 + (\alpha v_0^2 + \alpha^2 v_0 + 1)v_1 + \alpha v_0^2. \end{aligned}$$

Dividing $f(v_0, v_1)$ by $(\alpha v_0^2 + \alpha^2 v_0 + 1)^2/(v_0^2 + \alpha v_0 + 1)$ one gets the following equation

$$T^2 + T = \frac{v_0^2(v_0^2 + \alpha v_0 + 1)}{\alpha(v_0 + 1)^2(v_0 + \alpha^2)^2},$$

where

$$T = \frac{v_1(v_0^2 + \alpha v_0 + 1)}{\alpha(v_0 + 1)(v_0 + \alpha^2)}.$$

We define the tower $\mathcal{G}' = (G'_n)_{n \geq 0}$ where $G'_0 = \mathbb{F}_4(v_0)$ and for $n \geq 0$, $G'_{n+1} = G'_n(z_{n+1})$ where

$$z_{n+1}^2 + z_{n+1} = \frac{v_n^2(v_n^2 + \alpha v_n + 1)}{\alpha(v_n + 1)^2(v_n + \alpha^2)^2} \tag{6.2}$$

and

$$v_{n+1} = \frac{\alpha(v_n + 1)(v_n + \alpha^2)z_{n+1}}{v_n^2 + \alpha v_n + 1}.$$

By Artin-Schreier extension, at the first level G'_1/G'_0, there are two totally ramified places of different exponent 2, namely $(v_0 = 1)|(v_1 = 1)$ and $(v_0 = \alpha^2)|(v_1 = \alpha^2)$. Exploring the ramification locus by backward substitution, we have

$$\mathrm{Ram}(\mathcal{G}/G'_0) = \{(v_0 = \gamma) \mid \gamma \in \{0, 1, \alpha, \alpha^2\}\}.$$

More precisely, by using Magma computation we get the ramification at the first two levels as in Figure 6.1.

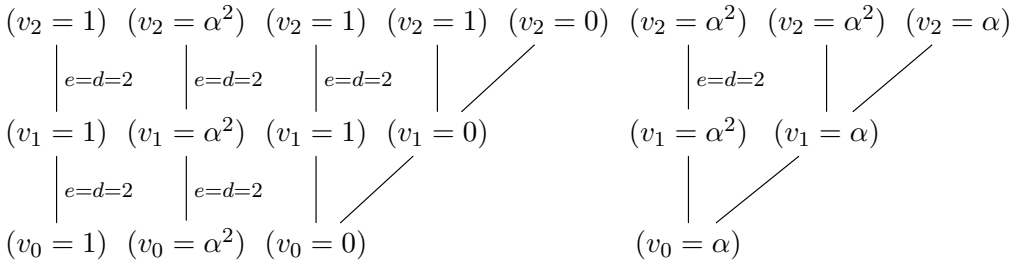

Figure 6.1: Ramification at the first two levels. Along the ramified places, we denote by e, d their ramification index and their different exponent, respectively.

So we have G'_{n+1}/G'_n is weakly ramified for $n = 0, 1$; i.e., $d = 2(e-1)$. Then by [Sti09, Remark 7.4.11.], the tower $\mathcal{G}'$ is 2-bounded.

Noticing that $g(G'_1) = 1$, we can give an upper bound for the genus by Hurwitz genus formula for $n \geq 1$.

$$\begin{aligned} 2g_n - 2 &= [G'_n : G'_1](2g_1 - 2) + \deg\mathrm{Diff}(G'_n/G'_1) \\ 2g_n - 2 &\leq 0 + 6 \cdot 2 \cdot [G'_n : G'_1] \\ g_n &\leq 6 \cdot 2^{n-1} + 1. \end{aligned}$$

Again, for having many rational places we consider the tower over $\mathbb{F}_{q^{2de}} = \mathbb{F}_{16}$. Assume that β is a primitive element of $\mathbb{F}_{16}$ (in particular $\alpha = \beta^5$). The following splitting locus is

$$\mathrm{Split}(\mathcal{G}'/G'_0) = \{(v_0 = \gamma) \mid \gamma \in \{\infty, \beta, \beta^2, \beta^4, \beta^6, \beta^7, \beta^8, \beta^9, \beta^{13}\}\}.$$

The number of rational places is bounded as

$$\begin{aligned} N(G'_n) &\geq \#\ \mathrm{Split}(\mathcal{G}'/G'_0) \cdot [G'_n : G'_0] \\ &\geq 9 \cdot 2^n \text{ for } n \geq 0. \end{aligned}$$

Finally, we observe that the tower $\mathcal{G}'$ is optimal over $\mathbb{F}_{16}$ since

$$\lambda(\mathcal{G}'/\mathbb{F}_{16}) = \lim_{n\to\infty} \frac{N(G'_n)}{g_n} \geq \lim_{n\to\infty} \frac{9 \cdot 2^n}{6 \cdot 2^{n-1} + 1} = 3 = \sqrt{16} - 1.$$

Since Tower $\mathcal{G}$ defines exactly the Drinfeld modular curves $(x_0(\mathfrak{p}^i))_{i\geq 0}$, its limit can be estimated $\lambda(\mathcal{G}) \geq q^d - 1 = 1$ by Theorem 4.5. Though derived from Tower $\mathcal{G}$, Tower $\mathcal{G}'$ is defined differently: its recursive representation (6.2) is not 'twisted' like the definition (6.1) of Tower $\mathcal{G}$. It not clear from the theory of Drinfeld modules why $\lambda(\mathcal{G}/\mathbb{F}_{16}) \geq 1$ but $\lambda(\mathcal{G}'/\mathbb{F}_{16}) \geq 3$.

6.2 Good towers from Drinfeld modules of rank 3

In Chapter 4 the theory of Drinfeld modular curves $x_0(\mathfrak{n})$ over general rings A and values of δ to construct good towers was investigated. As an example, a new explicit tower over $\mathbb{F}_{2^8}$ was constructed from rank 2 Drinfeld A-modules with $A \neq \mathbb{F}_q[T]$. In this section, we expand the construction for a special class of rank 3 Drinfeld A-modules over the same ring A. As a result we successfully construct a good tower over $\mathbb{F}_{2^6}$ with limit $3/2$.

In general, there is no notion of Drinfeld modular curves $x_0(\mathfrak{n})$ for Drinfeld modules of rank $r > 2$. In [BBGS15], by using a special class of Drinfeld $\mathbb{F}_q[T]$-modules, Bassa, Beelen, Garcia and Stichtenoth gave somehow such kind of Drinfeld modular curves for any rank $r \geq 2$. They used that to give the modularity for their tower. More precisely, they considered rank r Drinfeld $\mathbb{F}_q[T]$-modules of characteristic $T - 1$ of form

$$\phi_T = -\tau^r + g\tau^j + 1 \tag{6.3}$$

where $1 \leq j \leq r$. In our example when $A \neq \mathbb{F}_q[T]$, it is less immediate which kind of rank 3 Drinfeld A-modules can be used.

We use the same setting in Section 6.1 (the same ring A, the characteristic $P = \langle X, Y\rangle$, $\iota(X) = \iota(Y) = 0$, $\mathfrak{p} = \langle X - 1, Y\rangle$, $\mathfrak{p}$-isogeny $\lambda = \tau - a$). We consider a rank 3 Drinfeld A-module ϕ of form

$$\begin{aligned}\phi_X &= g_0\tau^6 + g_1\tau^5 + g_2\tau^4 + g_3\tau^3 + g_4\tau^2 + g_5\tau,\\ \phi_Y &= h_0\tau^6 + h_1\tau^5 + h_2\tau^4 + h_3\tau^3 + h_4\tau^2 + h_5\tau.\end{aligned}$$

The rank 3 Drinfeld module ϕ can also be normalized by putting $h_0 = 1$ and $g_0 \in \mathbb{F}_4$ satisfying $g_0^2 + g_0 + 1 = 0$. The variables g_i, h_j for $i, j \in$

$\{1, 2, ..., 5\}$ satisfy the linearized relations coming from the curve equation, $\phi_{Y^2+XY+X^2-X} = \phi_0 = 0$, and from the commutative property between X and Y, $\phi_X\phi_Y = \phi_{XY} = \phi_{YX} = \phi_Y\phi_X$. As a result, all variables g_i can be expressed in terms of h_i's for $i \in \{1, 2, ..., 5\}$.

In the case of rank $r = 2$ as in Chapter 4 or Section 6.1, the genus formula 4.8 for the curve $x(1)$ tells us when isomorphism classes of such a rank 2 Drinfeld module can be parametrized in one variable for recursively defined towers. More precisely, the setting in Section 4.5 with $F = \mathbb{F}_q(T)$ and $\delta = 2$ fitted the conditions for $g(x(1)) = 0$. The case of rank $r > 2$ has not been fully investigated in any ring A yet. Part of such an investigation for $A = \mathbb{F}_q[T]$ just has been explored in [BBGS15] where the considered rank r Drinfeld modules are of form 6.3 parametrized by only one variable g. In order to be able to parametrize isomorphism classes of our rank 3 Drinfeld module ϕ in one variable with high possibility, we set low-degree coefficients of ϕ_X and ϕ_Y, which are in this case g_5 and h_5, zeroes. Following the same elimination technique in Section 4.5, we can now reduce four variables $h_1, ..., h_4$ into two of them.

Everything then goes exactly the same as the construction in Section 4.5. Finally, we can also obtain two twisted polynomials to define the tower $\mathcal{F}' = (F'_0, F'_1, \cdots)$ starting with $F'_0 = \mathbb{F}_4(u_0)$.

$$\begin{aligned}
\Phi^1(u,v) &= (u+g_0)v^7 + (g_0u^3+u^2+g_0u+g_0)v^6 + (u^5+u^4+u^3+g_0u^2+g_0u \\
&\quad + g_0)v^5 + (u^7+g_0u^6+u^5+g_0^2u^4+g_0u^3+u^2+g_0^2u+g_0)v^4 + (u^6+g_0^2u^5 \\
&\quad + g_0u^4+u^3+g_0^2u^2+u+g_0)v^3 + (g_0u^5+g_0^2u^3+u^2+g_0^2u+g_0)v^2 + (g_0u^6 \\
&\quad + u^4+u^3+u+g_0)v + g_0^2u^7+g_0u^6+u^5+g_0^2u^4+g_0u^3+u^2+g_0^2u+g_0; \\
\Phi^2(v,w) &= (v+g_0^2)w^7 + (g_0^2v^3+v^2+g_0^2v+g_0^2)w^6 + (v^5+v^4+v^3+g_0^2v^2+g_0^2v \\
&\quad + g_0^2)w^5 + (v^7+g_0^2v^6+v^5+g_0v^4+g_0^2v^3+v^2+g_0v+g_0^2)w^4 + (v^6+g_0v^5 \\
&\quad + g_0^2v^4+v^3+g_0v^2+v+g_0^2)w^3 + (g_0^2v^5+g_0v^3+v^2+g_0v+g_0^2)w^2 + (g_0^2v^6 \\
&\quad + v^4+v^3+v+g_0^2)w + g_0v^7+g_0^2v^6+v^5+g_0v^4+g_0^2v^3+v^2+g_0v+g_0^2.
\end{aligned}$$

By computer we can see that Φ^i is not absolutely irreducible for $i = 1, 2$. It is irreducible only over $\mathbb{F}_4$. In order to define the tower from F'_2/F'_1

we have to pick one of its irreducible factors at each step. That produces several towers $\mathcal{F}'$.

In particular, F_2'/F_1' can be of degree 3 or degree 4, since $\Phi^2(u_1, u_2)$ has one factor of degree 3 and the other of degree 4 in $F_1'[u_2]$. If we choose the degree 4 for F_2'/F_1', there will be also either of degree 3 or degree 4 for F_3'/F_2'. If degree 3 is chosen for F_2'/F_1', then F_3'/F_2' could be of degree 1, of degree 2 or of degree 4. Next, if degree 2 is chosen for F_3'/F_2' then the degrees 1, 2 and 4 are repeated for F_4'/F_3', and so on. Such an exploration can be computed by using Magma.

We pick one instance of Tower $\mathcal{F}' = (F_0', F_1', ...)$ of degrees 7-3-2-2-$\cdots$ to compute the limit.

For having many rational places, we consider the tower defined over $\mathbb{F}_{q^{3de}} = \mathbb{F}_{2^6}$. Let α be a primitive element of $\mathbb{F}_{2^6}$, we choose $g_0 = \alpha^{21}$ such that $g_0^2 + g_0 + 1 = 0$. By Kummer's theory, ramified places at the first level F_1'/F_0' are $(u_0 = 0)$, $(u_0 = \infty)$ and $(u_0 = g_0)$. Afterwards, the place $(u_1 = 1)$ lying above $(u_0 = 0)$ splits completely.

We compute directly by Magma for first few levels and see that the field extension F_{n+1}'/F_n' is weakly ramified for $n = 0, 1, 2$; i.e., $d(P_{n+1}|P_n) = 2(e(P_{n+1}|P_n) - 1)$ where P_n denotes a place of function field F_n' for $n \geq 0$. Then by [Sti09, Remark 7.4.11.], the tower $\mathcal{F}'$ is 2-bounded. There are 10 places of degree 1 and 4 places of degree 2 in $\mathrm{Ram}(\mathcal{F}'/F_2')$. In summary we get the following upper bound for the genus of the function field F_n' in the tower $\mathcal{F}'$.

$$\begin{aligned} 2g(F_n') - 2 &= [F_n' : F_2'](2g(F_2') - 2) + \deg\mathrm{Diff}(F_n'/F_2') \\ 2g(F_n') - 2 &\leq 2^{n-2}(2 \cdot 13 - 2) + 2(10 \cdot 1 + 4 \cdot 2)2^{n-2} \\ g(F_n') &\leq 30 \cdot 2^{n-2} + 1 \text{ for } n \geq 2. \end{aligned}$$

As the places $(u_0 = g_0^2)$ and $(u_0 = 1)$ split completely in F_n' for $n \geq 1$, and $(u_1 = 1)$ splits completely in F_n' for $n \geq 2$, we get

$$N(F_n') \geq 2[F_n' : F_0] + [F_n' : F_1] = (2 \cdot 7 + 1) \cdot 3 \cdot 2^{n-2} = 45 \cdot 2^{n-2} \text{ for } n \geq 2.$$

As a result, we observe that the tower is good with limit

$$\lambda(\mathcal{F}) = \lim_{n \to \infty} \frac{N(F_n)}{g(F_n)} \geq \frac{45}{30} = 3/2.$$

6.3 The Hasse–Witt invariant in towers

For applications in coding theory, towers of function fields with a positive limit are useful. Subsequently, other applications of such towers in coding theory and cryptography were discovered, for instance for the construction of hash functions, low discrepancy sequences, secret sharing and multiparty computation. Specifically in some of these new applications additional properties of towers with positive limits are sometimes required. More precisely, for the construction of strongly multiplicative linear secret sharing schemes with positive asymptotic corruption tolerance rate, and the construction of fast bilinear multiplication algorithms in large extensions of a given finite field (see [CCX14]), one is also interested in the so-called p-rank of the function fields occurring in the tower.

The *p-rank* $\gamma(F)$ of a function field F with constant field $\overline{\mathbb{F}}_p$, the algebraic closure of the finite field $\mathbb{F}_p$, is defined as the dimension over $\mathbb{F}_p$ of the group of divisor classes of degree zero of order p. If the function field is defined over the finite field $\mathbb{F}_q$, we define its p-rank as the p-rank of the function field $F\overline{\mathbb{F}}_q$, obtained by extending the constant field to the algebraic closure of $\mathbb{F}_q$. It can be shown that $0 \leq \gamma(F) \leq g(F)$. If $\gamma(F) = g(F)$, then F is called *ordinary*. For a tower $\mathcal{F} = (F_n)_{n\geq 0}$, we consider the asymptotic behaviour of the ratio $\gamma(F_n)/g(F_n)$ when $g(F_n) \to \infty$ as

$$0 \leq \varphi(\mathcal{F}) := \liminf_{n\to\infty} \frac{\gamma(F_n)}{g(F_n)} \leq 1.$$

For applications in cryptography and coding theory mentioned above, explicit towers with big limit $\lambda(\mathcal{F})$ and small 'p-rank' $\varphi(\mathcal{F})$ are interesting. If q is a square then there exists an optimal tower $\mathcal{F}/\mathbb{F}_q$ (see [CCX14, BB10]) such that

$$\varphi(\mathcal{F}) = \frac{1}{\sqrt{q}+1}. \tag{6.4}$$

In [CCX14, BB10], the tower of Garcia and Stichtenoth [GS95] was used to prove Equality (6.4). It is the best known bound for the p-rank over square finite fields. For non-square finite fields, very few results are known

for the p-rank of good towers. Only for the tower over cubic finite fields introduced by Bassa, Garcia and Stichtenoth denoted by BaGS [BGS08], the p-rank has been computed in [BB10]. More precisely, for $q = p^{3e}$ the p-rank of the BaGS tower is equal to

$$\varphi(\mathrm{BaGS}/\mathbb{F}_q) = \frac{2\binom{p+1}{2}^e - 2}{(p^e-1)(p^e+2)}, \tag{6.5}$$

where $\binom{\cdot}{\cdot}$ denotes the binomial coefficient. In particular, the tower is ordinary if $e = 1$.

Computing the p-rank of a tower is a quite difficult task. It is usually required that such a good tower should have p-Galois steps and precise ramification in order to apply Deuring–Shafarevich theorem to compute the p-rank. Very few good towers like towers Garcia-Stichtenoth [GS95] or BaGS [BGS08] have such nice properties. Recently, a new explicit tower over any non-prime finite fields $\mathbb{F}_{q^n}$ has been introduced in [BBGS15], where a tower $\mathcal{F}$ was addressed and recursively defined by

$$\frac{Y^{q^n-1}-1}{Y^{q^j-1}} = \frac{X^{q^n-1}-1}{X^{q^n-q^k}},$$

with $n = j + k$ and $\gcd(j, k) = 1$. Over cubic finite fields; i.e., $n = 3$, a variant of this tower $\mathcal{F}$ has Galois steps; and hence its p-rank can hopefully be computed.

In order to compute the p-rank of a tower, we need to investigate the ramification structure and compute the genus of the tower. In Chapter 5, a subtower $\mathcal{Z} = (\mathbb{F}_{q^3}(z_1, ..., z_i))_{i\geq 1}$ of Tower $\mathcal{F} = (\mathbb{F}_{q^3}(x_1, ..., x_i))_{i\geq 1}$ was fully investigated. Their relationship is given by $z_i = x_i^{q^3-1}$ (see [BBGS15]); that helps in investigating the ramification structure and computing the genus of the tower $\mathcal{F}$. It seems that the p-rank of this tower $\mathcal{F}$ is smaller than the one of BaGS. In fact, in our current work we can compute the p-rank of the tower $\mathcal{F}/\mathbb{F}_{p^3}$ as

$$\varphi(\mathcal{F}/\mathbb{F}_{p^3}) = \lim_{n\to\infty} \frac{\gamma(F_n)}{g(F_n)} = \frac{p^2+p+4}{4(p^2+p+1)}. \tag{6.6}$$

So, this tower is not ordinary when $q = p^3$.

6.4 Drinfeld modular curves having many points

In recent years there has been renewed interest in the construction of curves over finite fields $\mathbb{F}_q$ with many rational points. We refer to [man] for a long list of references and for a table with the known records in the genus range $g \leq 50$ and small q's. Admittedly, the fact that a sequence of curves is asymptotically optimal implies literally nothing for an individual curve from this sequence. But morally it is a good candidate for a curve with many points. It seems that reductions of Drinfeld modular curves $X_0(\mathfrak{n})$ have not been investigated under this aspect before, and it looks as if they do in general not give the best results.

In general it is not easy to write down an equation for a Drinfeld modular curve even in the simplest case of $A = \mathbb{F}_q[T]$. But the moduli interpretation allows to predict certain rational points on it. In fact, most rational points are supersingular. There are also some rational cusps. Others are rare and not easy to determine. In the case of $A = \mathbb{F}_q[T]$, Gekeler gave the formula to compute the number of supersingular points and a lower bound for the rational cusps of the Drinfeld modular curves $X_0(\mathfrak{n})$. Schweizer showed in [Sch02] by using such formulas that the reduction of Drinfeld modular curve $X_0(T^3(T+1)^2)$ modulo $T-1$ has genus 42 and has at least 122 rational points over $\mathbb{F}_{3^2}$. For that it appeared on the table [man] as one of the best known curves.

In Chapter 3 and Chapter 4 we obtained somehow an algorithm to write down an explicit equation for a Drinfeld modular curve $X_0(\mathfrak{n})$. This can help not only to check Gekeler's formulas but also to find the exact number of rational points of $X_0(\mathfrak{n})$ so that it can produce certain best curves.

Appendix A

Magma source code

This Appendix gives the Magma sources with outputs of computational verifications in Section 4.5.

1. Producing relations between the variables from $\phi_{Y^2+XY+X^2-X} = 0$ and $\phi_X\phi_Y = \phi_Y\phi_X$.

```
/* 1_normalize_phi.txt */
/*
Define a normalized rank-2 Drinfeld module over the coefficient ring of the curve
Y^2 + aXY + bX^2 = X over GF(q)
*/
q:=2;
FX<X>:=GF(q,2);
P<Y>:=PolynomialRing(FX);

/*
in GF(2) only a = b = 1 satisfies T^2 + aT + b is irreducible
*/
a := 1; b := 1;
f:=Y^2 + a*X*Y + b*X^2 - X;

C<Y>:=ext<FX|f>;

L<g0,g1,g2,g3,h0,h1,h2,h3>:=PolynomialRing(C,8);
```

```
F<tau>:=TwistedPolynomials(L);
phiX:=F![X,g3,g2,g1,g0];
phiY:=F![Y,h3,h2,h1,h0];
/*
phiX = g0*tau^4 + g1*tau^3 + g2*tau^2 + g3*tau + X
phiY = h0*tau^4 + h1*tau^3 + h2*tau^2 + h3*tau + Y
*/
phiXY:=phiX*phiY;
phiX2:=phiX*phiX;
phiY2:=phiY*phiY;
phiCurve:= phiY2 + F![a]*phiXY + F![b]*phiX2 - phiX;
Curve:=Polynomial(phiCurve);
L1:=Eltseq(phiCurve);

phiYX:=phiY*phiX;
phiCommute:=phiXY-phiYX;
L2:=Eltseq(phiCommute);
/*
L1 = relations from phi_{Y^2 + XY + X^2 - X} = 0
[
    0,
    (X*Y + 1)*g3 + (X^2*Y + X^2)*h3,
    (Y + X^2)*g2 + g3^3 + g3*h3^2 + h3^3,
    (X*Y + X)*g1 + g2^2*g3 + g2*g3^4 + g2*h3^4 + g3*h2^2 + X^2*Y*h1 + h2^2*h3 +
        h2*h3^4,
    (Y + 1)*g0 + g1^2*g3 + g1*g3^8 + g1*h3^8 + g2^5 + g2*h2^4 + g3*h1^2 + X*h0 +
        h1^2*h3 + h1*h3^8 + h2^5,
    g0^2*g3 + g0*g3^16 + g0*h3^16 + g1^4*g2 + g1*g2^8 + g1*h2^8 + g2*h1^4 +
        g3*h0^2 + h0^2*h3 + h0*h3^16 + h1^4*h2 + h1*h2^8,
    g0^4*g2 + g0*g2^16 + g0*h2^16 + g1^9 + g1*h1^8 + g2*h0^4 + h0^4*h2 +
        h0*h2^16 + h1^9,
    g0^8*g1 + g0*g1^16 + g0*h1^16 + g1*h0^8 + h0^8*h1 + h0*h1^16,
    g0^17 + g0*h0^16 + h0^17
]
L2 = relations from phi_XY = phi_YX
[
    0,
    (X^2*Y + 1)*g3 + h3,
    X*g2 + g3^2*h3 + g3*h3^2,
    (X^2*Y + X)*g1 + g2^2*h3 + g2*h3^4 + g3^4*h2 + g3*h2^2 + h1,
    g1^2*h3 + g1*h3^8 + g2^4*h2 + g2*h2^4 + g3^8*h1 + g3*h1^2,
    g0^2*h3 + g0*h3^16 + g1^4*h2 + g1*h2^8 + g2^8*h1 + g2*h1^4 + g3^16*h0 +
        g3*h0^2,
    g0^4*h2 + g0*h2^16 + g1^8*h1 + g1*h1^8 + g2^16*h0 + g2*h0^4,
    g0^8*h1 + g0*h1^16 + g1^16*h0 + g1*h0^8,
    g0^16*h0 + g0*h0^16
]

*/

lp:=GCD(L1[#L1],L2[#L2]);
/*
g0^2 + g0*h0 + h0^2
we can choose h0 = 1 for normalized Drinfeld modules. Then g0^2 + g0 + 1 = 0.
Recall that X^2 + X + 1 = 0. We will see that g0 = X or g0 = X^2
```

```
corresponds to 2 components of X(1) later.
*/
L1:=L1[1..#L1-1];
L2[#L2]:=lp;

for i in [1..#L1] do
    L1[i]:=Evaluate(L1[i],5,1);
end for;

for i in [1..#L2] do
    L2[i]:=Evaluate(L2[i],5,1);
end for;

/*
[
    0,
    (X*Y + 1)*g3 + (X^2*Y + X^2)*h3,
    (Y + X^2)*g2 + g3^3 + g3*h3^2 + h3^3,
    (X*Y + X)*g1 + g2^2*g3 + g2*g3^4 + g2*h3^4 + g3*h2^2 + X^2*Y*h1 + h2^2*h3 +
        h2*h3^4,
    (Y + 1)*g0 + g1^2*g3 + g1*g3^8 + g1*h3^8 + g2^5 + g2*h2^4 + g3*h1^2 +
        h1^2*h3 + h1*h3^8 + h2^5 + X,
    g0^2*g3 + g0*g3^16 + g0*h3^16 + g1^4*g2 + g1*g2^8 + g1*h2^8 + g2*h1^4 + g3 +
        h1^4*h2 + h1*h2^8 + h3^16 + h3,
    g0^4*g2 + g0*g2^16 + g0*h2^16 + g1^9 + g1*h1^8 + g2 + h1^9 + h2^16 + h2,
    g0^8*g1 + g0*g1^16 + g0*h1^16 + g1 + h1^16 + h1
]
[
    0,
    (X^2*Y + 1)*g3 + h3,
    X*g2 + g3^2*h3 + g3*h3^2,
    (X^2*Y + X)*g1 + g2^2*h3 + g2*h3^4 + g3^4*h2 + g3*h2^2 + h1,
    g1^2*h3 + g1*h3^8 + g2^4*h2 + g2*h2^4 + g3^8*h1 + g3*h1^2,
    g0^2*h3 + g0*h3^16 + g1^4*h2 + g1*h2^8 + g2^8*h1 + g2*h1^4 + g3^16 + g3,
    g0^4*h2 + g0*h2^16 + g1^8*h1 + g1*h1^8 + g2^16 + g2,
    g0^8*h1 + g0*h1^16 + g1^16 + g1,
    g0^2 + g0 + 1
]

*/
for i in [2..5] do
L1[i]:=Factorization(L1[i])[1][1];
end for;
/*
[
    0,
    g3 + X*Y*h3,
    g2 + (X^2*Y + X^2)*g3^3 + (X^2*Y + X^2)*g3*h3^2 + (X^2*Y + X^2)*h3^3,
    g1 + (X*Y + 1)*g2^2*g3 + (X*Y + 1)*g2*g3^4 + (X*Y + 1)*g2*h3^4 + (X*Y +
        1)*g3*h2^2 + (Y + 1)*h1 + (X*Y + 1)*h2^2*h3 + (X*Y + 1)*h2*h3^4,
    g0 + (X^2*Y + X)*g1^2*g3 + (X^2*Y + X)*g1*g3^8 + (X^2*Y + X)*g1*h3^8 +
        (X^2*Y + X)*g2^5 + (X^2*Y + X)*g2*h2^4 + (X^2*Y + X)*g3*h1^2 + (X^2*Y +
        X)*h1^2*h3 + (X^2*Y + X)*h1*h3^8 + (X^2*Y + X)*h2^5 + Y + X^2,
    g0^2*g3 + g0*g3^16 + g0*h3^16 + g1^4*g2 + g1*g2^8 + g1*h2^8 + g2*h1^4 + g3 +
        h1^4*h2 + h1*h2^8 + h3^16 + h3,
```

```
    g0^4*g2 + g0*g2^16 + g0*h2^16 + g1^9 + g1*h1^8 + g2 + h1^9 + h2^16 + h2,
    g0^8*g1 + g0*g1^16 + g0*h1^16 + g1 + h1^16 + h1
]
[
    0,
    (X^2*Y + 1)*g3 + h3,
    X*g2 + g3^2*h3 + g3*h3^2,
    (X^2*Y + X)*g1 + g2^2*h3 + g2*h3^4 + g3^4*h2 + g3*h2^2 + h1,
    g1^2*h3 + g1*h3^8 + g2^4*h2 + g2*h2^4 + g3^8*h1 + g3*h1^2,
    g0^2*h3 + g0*h3^16 + g1^4*h2 + g1*h2^8 + g2^8*h1 + g2*h1^4 + g3^16 + g3,
    g0^4*h2 + g0*h2^16 + g1^8*h1 + g1*h1^8 + g2^16 + g2,
    g0^8*h1 + g0*h1^16 + g1^16 + g1,
    g0^2 + g0 + 1
]
*/
/*
express other variables in h1,h2,h3
*/
temp:=g3 - L1[2];
for i in [3..#L1] do
    L1[i]:=Evaluate(L1[i],4,temp);
end for;
for i in [2..#L2] do
    L2[i]:=Evaluate(L2[i],4,temp);
end for;

temp:=g2 - L1[3];
for i in [4..#L1] do
    L1[i]:=Evaluate(L1[i],3,temp);
end for;
for i in [2..#L2] do
    L2[i]:=Evaluate(L2[i],3,temp);
end for;

temp:=g1 - L1[4];
for i in [5..#L1] do
    L1[i]:=Evaluate(L1[i],2,temp);
end for;
for i in [2..#L2] do
    L2[i]:=Evaluate(L2[i],2,temp);
end for;

temp:=g0 - L1[5];
for i in [6..#L1] do
    L1[i]:=Evaluate(L1[i],1,temp);
end for;
for i in [2..#L2] do
    L2[i]:=Evaluate(L2[i],1,temp);
end for;

L1;L2;
/*
[
    0,
    g3 + X*Y*h3,
```

```
    g2 + (X*Y + X)*h3^3,
    g1 + (Y + 1)*h1 + (Y + X)*h2^2*h3 + (X*Y + 1)*h2*h3^4 + h3^7,
    g0 + (X^2*Y + 1)*h1^2*h3 + (X*Y + X)*h1*h3^8 + (X^2*Y + X)*h2^5 + (X^2*Y +
        X)*h2^4*h3^3 + (X*Y + 1)*h2^2*h3^9 + X*h2*h3^12 + Y*h3^15 + Y + X^2,
    h1^4*h2 + Y*h1^4*h3^3 + X*h1^2*h3^17 + Y*h1*h2^8 + (Y + X)*h1*h3^24 + (Y +
        X^2)*h2^10*h3 + (X*Y + 1)*h2^9*h3^4 + (Y + X)*h2^8*h3^7 + (X*Y +
        X^2)*h2^5*h3^16 + (X^2*Y + 1)*h2^4*h3^19 + X*Y*h2^2*h3^25 + (X*Y +
        X)*h2*h3^28 + (X*Y + 1)*h3^31 + X^2*Y*h3^16 + (X*Y + X)*h3,
    (X^2*Y + 1)*h1^9 + (X*Y + 1)*h1^8*h2^2*h3 + h1^8*h2*h3^4 + (Y +
        X^2)*h1^8*h3^7 + h1^4*h3^35 + (X^2*Y + 1)*h1^2*h2^16*h3 + (Y +
        X^2)*h1^2*h3^49 + (X*Y + 1)*h1*h2^16*h3^8 + (X^2*Y + 1)*h1*h2^8*h3^32 +
        h1*h3^56 + (X^2*Y + X)*h2^21 + (Y + X)*h2^20*h3^3 + (X^2*Y +
        1)*h2^18*h3^9 + Y*h2^17*h3^12 + (Y + 1)*h2^16*h3^15 + (Y + X)*h2^16 +
        h2^10*h3^33 + (X*Y + X)*h2^9*h3^36 + X*h2^5*h3^48 + (X^2*Y +
        1)*h2^4*h3^51 + (Y + X^2)*h2^2*h3^57 + (Y + X)*h2*h3^60 + h2 + (X^2*Y +
        X)*h3^63 + X^2*h3^48 + (Y + X)*h3^3,
    X^2*h1^18*h3 + (Y + X^2)*h1^17*h3^8 + (X^2*Y + X^2)*h1^16*h2^5 + (X^2*Y +
        X^2)*h1^16*h2^4*h3^3 + X*h1^16*h2^2*h3^9 + X^2*h1^16*h2*h3^12 + (Y +
        X^2)*h1^16*h3^15 + Y*h1^16 + (Y + X^2)*h1^9*h3^64 + (X*Y +
        X)*h1^8*h2^2*h3^65 + Y*h1^8*h2*h3^68 + (Y + X)*h1^8*h3^71 + (Y +
        1)*h1^2*h2^32*h3^17 + X^2*Y*h1^2*h2^16*h3^65 + (X^2*Y + 1)*h1^2*h3^113 +
        (X*Y + X^2)*h1*h2^40 + X*h1*h2^32*h3^24 + X^2*Y*h1*h2^16*h3^72 + (X^2*Y
        + X^2)*h1*h2^8*h3^96 + (Y + X)*h1*h3^120 + X*h1 + X^2*h2^42*h3 + (Y +
        1)*h2^41*h3^4 + X^2*Y*h2^40*h3^7 + X*Y*h2^37*h3^16 + X*Y*h2^36*h3^19 +
        (Y + X^2)*h2^34*h3^25 + (X^2*Y + X)*h2^33*h3^28 + (X^2*Y +
        1)*h2^32*h3^31 + X^2*Y*h2^32*h3^16 + (X*Y + X^2)*h2^21*h3^64 + (X*Y +
        X^2)*h2^20*h3^67 + (Y + X^2)*h2^18*h3^73 + Y*h2^17*h3^76 + (X^2*Y +
        X)*h2^16*h3^79 + (X^2*Y + 1)*h2^16*h3^64 + (X^2*Y + 1)*h2^10*h3^97 + (Y
        + X^2)*h2^9*h3^100 + X^2*h2^8*h3^103 + (X^2*Y + X)*h2^5*h3^112 + (X^2*Y
        + X)*h2^4*h3^115 + Y*h2^2*h3 + X^2*h2*h3^124 + (Y + X)*h2*h3^4 + (X^2*Y
        + X)*h3^127 + (Y + X^2)*h3^112 + (X*Y + 1)*h3^7
]
[
    0,
    0,
    0,
    0,
    0,
    (Y + X^2)*h1^4*h2 + (Y + 1)*h1^4*h3^3 + (X*Y + 1)*h1^2*h3^17 + (Y +
        1)*h1*h2^8 + X^2*Y*h1*h3^24 + (X*Y + X^2)*h2^10*h3 + (X^2*Y +
        1)*h2^9*h3^4 + X^2*Y*h2^8*h3^7 + Y*h2^5*h3^16 + X*Y*h2^4*h3^19 + (X*Y +
        X)*h2^2*h3^25 + X^2*h2*h3^28 + (X^2*Y + 1)*h3^31 + (X^2*Y + X^2)*h3^16 +
        X^2*h3,
    (X^2*Y + X)*h1^9 + (Y + X)*h1^8*h2^2*h3 + (Y + 1)*h1^8*h2*h3^4 + h1^8*h3^7 +
        (X*Y + 1)*h1^4*h2*h3^32 + (X^2*Y + 1)*h1^2*h2^16*h3 + X^2*h1*h2^16*h3^8
        + Y*h1*h2^8*h3^32 + h1*h3^56 + h2^21 + (X^2*Y + X)*h2^20*h3^3 + (X*Y +
        1)*h2^18*h3^9 + (X^2*Y + 1)*h2^17*h3^12 + Y*h2^16*h3^15 + (Y +
        X^2)*h2^16 + (X*Y + X)*h2^9*h3^36 + X*h2^5*h3^48 + (Y + X)*h2*h3^60 + (Y
        + 1)*h2 + (X*Y + X)*h3^48 + (X*Y + X)*h3^3,
    (X^2*Y + 1)*h1^18*h3 + Y*h1^17*h3^8 + (X^2*Y + X)*h1^16*h2^5 + (X^2*Y +
        X)*h1^16*h2^4*h3^3 + (X*Y + 1)*h1^16*h2^2*h3^9 + X*h1^16*h2*h3^12 +
        Y*h1^16*h3^15 + X*h1^16 + (Y + X)*h1^9*h3^64 + X^2*Y*h1*h2^40 +
        X^2*Y*h1*h2^32*h3^24 + Y*h1*h2^16*h3^72 + X^2*h1*h2^8*h3^96 + (X*Y +
        X)*h1*h3^120 + (X^2*Y + 1)*h1 + (Y + X)*h2^32*h3^16 + (X*Y +
        1)*h2^16*h3^64 + (Y + X)*h2^2*h3 + (X*Y + 1)*h2*h3^4 + h3^112 + h3^7,
```

```
    (X^2*Y + X^2)*h1^4*h3^2 + Y*h1^2*h3^16 + (X^2*Y + 1)*h1^2*h3 + (X*Y +
        X)*h1*h3^8 + (X^2*Y + 1)*h2^10 + (X^2*Y + 1)*h2^8*h3^6 + (X^2*Y +
        X)*h2^5 + (Y + X)*h2^4*h3^18 + (X^2*Y + X)*h2^4*h3^3 + X^2*h2^2*h3^24 +
        (X*Y + 1)*h2^2*h3^9 + X*h2*h3^12 + (X*Y + 1)*h3^30 + Y*h3^15 + X^2*Y + 1
]

*/
```

2. Finding the relation $f(h_2, h_3) = 0$ using Groebner basis computation (elimination). The Groebner basis is stored in B.txt, whose the last element is $f(h_2, h_3)$.

```
/* 2_p_h2_h3.txt */
/*
finding relation between h2 and h3 using Groebner basis computation (elimination)
*/
q:=2;
FX<X>:=GF(q,2);
P<Y>:=PolynomialRing(FX);
f:=Y^2 + X*Y + X^2 - X;

C<Y>:=ext<FX|f>;
P<h1,h2,h3>:=PolynomialRing(C,3);
L:=[
    h1^4*h2 + Y*h1^4*h3^3 + X*h1^2*h3^17 + Y*h1*h2^8 + (Y + X)*h1*h3^24 + (Y +
        X^2)*h2^10*h3 + (X*Y + 1)*h2^9*h3^4 + (Y + X)*h2^8*h3^7 + (X*Y +
        X^2)*h2^5*h3^16 + (X^2*Y + 1)*h2^4*h3^19 + X*Y*h2^2*h3^25 + (X*Y +
        X)*h2*h3^28 + (X*Y + 1)*h3^31 + X^2*Y*h3^16 + (X*Y + X)*h3,
    (X^2*Y + 1)*h1^9 + (X*Y + 1)*h1^8*h2^2*h3 + h1^8*h2*h3^4 + (Y +
        X^2)*h1^8*h3^7 + h1^4*h3^35 + (X^2*Y + 1)*h1^2*h2^16*h3 + (Y +
        X^2)*h1^2*h3^49 + (X*Y + 1)*h1*h2^16*h3^8 + (X^2*Y + 1)*h1*h2^8*h3^32 +
        h1*h3^56 + (X^2*Y + X)*h2^21 + (Y + X)*h2^20*h3^3 + (X^2*Y +
        1)*h2^18*h3^9 + Y*h2^17*h3^12 + (Y + 1)*h2^16*h3^15 + (Y + X)*h2^16 +
        h2^10*h3^33 + (X*Y + X)*h2^9*h3^36 + X*h2^5*h3^48 + (X^2*Y +
        1)*h2^4*h3^51 + (Y + X^2)*h2^2*h3^57 + (Y + X)*h2*h3^60 + h2 + (X^2*Y +
        X)*h3^63 + X^2*h3^48 + (Y + X)*h3^3,
    X^2*h1^18*h3 + (Y + X^2)*h1^17*h3^8 + (X^2*Y + X^2)*h1^16*h2^5 + (X^2*Y +
        X^2)*h1^16*h2^4*h3^3 + X*h1^16*h2^2*h3^9 + X^2*h1^16*h2*h3^12 + (Y +
        X^2)*h1^16*h3^15 + Y*h1^16 + (Y + X^2)*h1^9*h3^64 + (X*Y +
        X)*h1^8*h2^2*h3^65 + Y*h1^8*h2*h3^68 + (Y + X)*h1^8*h3^71 + (Y +
        1)*h1^2*h2^32*h3^17 + X^2*Y*h1^2*h2^16*h3^65 + (X^2*Y + 1)*h1^2*h3^113 +
        (X*Y + X^2)*h1*h2^40 + X*h1*h2^32*h3^24 + X^2*Y*h1*h2^16*h3^72 + (X^2*Y
        + X^2)*h1*h2^8*h3^96 + (Y + X)*h1*h3^120 + X*h1 + X^2*h2^42*h3 + (Y +
        1)*h2^41*h3^4 + X^2*Y*h2^40*h3^7 + X*Y*h2^37*h3^16 + X*Y*h2^36*h3^19 +
        (Y + X^2)*h2^34*h3^25 + (X^2*Y + X)*h2^33*h3^28 + (X^2*Y +
        1)*h2^32*h3^31 + X^2*Y*h2^32*h3^16 + (X*Y + X^2)*h2^21*h3^64 + (X*Y +
        X^2)*h2^20*h3^67 + (Y + X^2)*h2^18*h3^73 + Y*h2^17*h3^76 + (X^2*Y +
        X)*h2^16*h3^79 + (X^2*Y + 1)*h2^16*h3^64 + (X^2*Y + 1)*h2^10*h3^97 + (Y
        + X^2)*h2^9*h3^100 + X^2*h2^8*h3^103 + (X^2*Y + X)*h2^5*h3^112 + (X^2*Y
        + X)*h2^4*h3^115 + Y*h2^2*h3 + X^2*h2*h3^124 + (Y + X)*h2*h3^4 + (X^2*Y
        + X)*h3^127 + (Y + X^2)*h3^112 + (X*Y + 1)*h3^7,
    (Y + X^2)*h1^4*h2 + (Y + 1)*h1^4*h3^3 + (X*Y + 1)*h1^2*h3^17 + (Y +
        1)*h1*h2^8 + X^2*Y*h1*h3^24 + (X*Y + X^2)*h2^10*h3 + (X^2*Y +
```

```
        1)*h2^9*h3^4 + X^2*Y*h2^8*h3^7 + Y*h2^5*h3^16 + X*Y*h2^4*h3^19 + (X*Y +
        X)*h2^2*h3^25 + X^2*h2*h3^28 + (X^2*Y + 1)*h3^31 + (X^2*Y + X^2)*h3^16 +
        X^2*h3,
    (X^2*Y + X)*h1^9 + (Y + X)*h1^8*h2^2*h3 + (Y + 1)*h1^8*h2*h3^4 + h1^8*h3^7 +
        (X*Y + 1)*h1^4*h2*h3^32 + (X^2*Y + 1)*h1^2*h2^16*h3 + X^2*h1*h2^16*h3^8
        + Y*h1*h2^8*h3^32 + h1*h3^56 + h2^21 + (X^2*Y + X)*h2^20*h3^3 + (X*Y +
        1)*h2^18*h3^9 + (X^2*Y + 1)*h2^17*h3^12 + Y*h2^16*h3^15 + (Y +
        X^2)*h2^16 + (X*Y + X)*h2^9*h3^36 + X*h2^5*h3^48 + (Y + X)*h2*h3^60 + (Y
        + 1)*h2 + (X*Y + X)*h3^48 + (X*Y + X)*h3^3,
    (X^2*Y + 1)*h1^18*h3 + Y*h1^17*h3^8 + (X^2*Y + X)*h1^16*h2^5 + (X^2*Y +
        X)*h1^16*h2^4*h3^3 + (X*Y + 1)*h1^16*h2^2*h3^9 + X*h1^16*h2*h3^12 +
        Y*h1^16*h3^15 + X*h1^16 + (Y + X)*h1^9*h3^64 + X^2*Y*h1*h2^40 +
        X^2*Y*h1*h2^32*h3^24 + Y*h1*h2^16*h3^72 + X^2*h1*h2^8*h3^96 + (X*Y +
        X)*h1*h3^120 + (X^2*Y + 1)*h1 + (Y + X)*h2^32*h3^16 + (X*Y +
        1)*h2^16*h3^64 + (Y + X)*h2^2*h3 + (X*Y + 1)*h2*h3^4 + h3^112 + h3^7,
    (X^2*Y + X^2)*h1^4*h3^2 + Y*h1^2*h3^16 + (X^2*Y + 1)*h1^2*h3 + (X*Y +
        X)*h1*h3^8 + (X^2*Y + 1)*h2^10 + (X^2*Y + 1)*h2^8*h3^6 + (X^2*Y +
        X)*h2^5 + (Y + X)*h2^4*h3^18 + (X^2*Y + X)*h2^4*h3^3 + X^2*h2^2*h3^24 +
        (X*Y + 1)*h2^2*h3^9 + X*h2*h3^12 + (X*Y + 1)*h3^30 + Y*h3^15 + X^2*Y + 1
];

I:=ideal<P|L>;
B:=GroebnerBasis(I);
Write("B.txt",B);
/*
the last polynomial in B.txt is in h2,h3
*/
```

3. Finding $p(h_{22}, h_{33})$ defining $X(1)$ and its two components p^1, p^2.

```
/* 3_p_h22_h33_X_1.txt */
/*
finding 2 components of X(1)
*/
q:=2;
FX<X>:=GF(q,2);
P<Y>:=PolynomialRing(FX);
f:=Y^2 + X*Y + X^2 - X;

C<Y>:=ext<FX|f>;
Q<h2,h3,h22,h33>:=PolynomialRing(C,4);
/*
pick the last one in the Groebner Basis B
*/
pol:=h2^30 + (X*Y + X)*h2^29*h3^3 + (Y + X)*h2^27*h3^9 + (X*Y + 1)*h2^26*h3^12 +
        (Y + 1)*h2^25 + (X*Y + X)*h2^24*h3^18 + (X^2*Y + X^2)*h2^24*h3^3 +
        Y*h2^23*h3^21 + (X^2*Y + 1)*h2^23*h3^6 + X^2*Y*h2^22*h3^9 + (X*Y +
        1)*h2^21*h3^27 + (X^2*Y + X)*h2^21*h3^12 + h2^20*h3^30 + (Y +
        1)*h2^20*h3^15 + (X*Y + 1)*h2^20 + (X^2*Y + X^2)*h2^19*h3^18 +
        Y*h2^18*h3^36 + (X*Y + X)*h2^18*h3^6 + (Y + X)*h2^17*h3^39 + (Y +
        X^2)*h2^17*h3^24 + X*h2^17*h3^9 + (X^2*Y + 1)*h2^16*h3^27 +
        X*Y*h2^16*h3^12 + h2^15*h3^45 + (Y + 1)*h2^15*h3^30 + X*Y*h2^15*h3^15 +
        (Y + X)*h2^15 + (X^2*Y + X^2)*h2^14*h3^33 + (Y + 1)*h2^14*h3^18 +
        h2^14*h3^3 + Y*h2^13*h3^51 + X*Y*h2^13*h3^36 + X*h2^13*h3^21 + (X*Y +
```

```
        X)*h2^13*h3^6 + (Y + X)*h2^12*h3^54 + X^2*Y*h2^12*h3^39 + (X^2*Y +
        X)*h2^12*h3^9 + (X^2*Y + X)*h2^11*h3^42 + (Y + X^2)*h2^11*h3^27 +
        X*h2^11*h3^12 + h2^10*h3^60 + (Y + X^2)*h2^10*h3^45 + X*h2^10*h3^30 + (Y
        + X)*h2^10*h3^15 + (X*Y + 1)*h2^10 + (X*Y + X)*h2^9*h3^63 +
        X^2*Y*h2^9*h3^48 + (X*Y + X)*h2^9*h3^33 + (X*Y + 1)*h2^9*h3^18 + (X*Y +
        X)*h2^9*h3^3 + X*Y*h2^8*h3^51 + (X^2*Y + X)*h2^8*h3^36 + (X*Y +
        X)*h2^8*h3^21 + (Y + X)*h2^8*h3^6 + (Y + X)*h2^7*h3^69 + (Y +
        X^2)*h2^7*h3^54 + (X^2*Y + 1)*h2^7*h3^39 + (X*Y + 1)*h2^7*h3^24 +
        X*h2^7*h3^9 + (X*Y + 1)*h2^6*h3^72 + X*Y*h2^6*h3^42 + (X*Y +
        1)*h2^6*h3^27 + (Y + X^2)*h2^6*h3^12 + X*h2^5*h3^60 + (X*Y +
        1)*h2^5*h3^45 + h2^5*h3^30 + (X*Y + X^2)*h2^5*h3^15 + (Y + 1)*h2^5 +
        (X*Y + X)*h2^4*h3^78 + Y*h2^4*h3^48 + (X^2*Y + X)*h2^4*h3^33 + (X*Y +
        X)*h2^4*h3^18 + X^2*h2^4*h3^3 + Y*h2^3*h3^81 + X*Y*h2^3*h3^66 +
        X*h2^3*h3^51 + (X^2*Y + X^2)*h2^3*h3^36 + X*Y*h2^3*h3^21 + (X*Y +
        X^2)*h2^2*h3^69 + (Y + X)*h2^2*h3^54 + (Y + 1)*h2^2*h3^39 + (Y +
        X)*h2^2*h3^24 + (Y + X^2)*h2^2*h3^9 + (X*Y + 1)*h2*h3^87 + h2*h3^57 +
        X^2*Y*h2*h3^42 + (X^2*Y + X^2)*h2*h3^27 + (X^2*Y + 1)*h2*h3^12 + h3^90 +
        X*h3^75 + h3^60 + X^2*h3^45 + X^2*h3^30 + 1;
/*
go to isomorphism classes: h22 = h2^(q^2+1), h33 = h3^((q^2+1)*(q+1))
*/
I:=ideal<Q|pol,h33-h3^((q^2+1)*(q+1)),h22 - h2^(q^2+1)>;
GB:=GroebnerBasis(I);
p:=GB[#GB];
/*
The last one p of GB defines Drinfeld modular curve X(1)
*/
Factorization(p);
/*
X(1) has two components
[
    <h22^15 + X*h22^14*h33 + (X^2*Y + 1)*h22^14 + X*h22^13*h33^2 + (Y +
        X)*h22^13*h33 + (X^2*Y + X^2)*h22^13 + X^2*h22^12*h33^3 + (X^2*Y +
        1)*h22^12*h33^2 + (X*Y + 1)*h22^12 + X^2*h22^11*h33^4 + (X^2*Y +
        X^2)*h22^11*h33^2 + X^2*Y*h22^11 + h22^10*h33^5 + (Y + X)*h22^10*h33^4 +
        (X*Y + X)*h22^10*h33^3 + (X*Y + 1)*h22^10*h33^2 + X*h22^10 + h22^9*h33^6
        + (X*Y + X^2)*h22^9*h33^5 + (X*Y + X)*h22^9*h33^4 + X^2*Y*h22^9*h33^2 +
        X*h22^9*h33 + (Y + X)*h22^9 + X*h22^8*h33^7 + (X*Y + X^2)*h22^8*h33^6 +
        (X*Y + X)*h22^8*h33^5 + (Y + X^2)*h22^8*h33^4 + X^2*Y*h22^8*h33^3 +
        h22^8*h33^2 + (X*Y + X^2)*h22^8*h33 + (Y + 1)*h22^8 + X^2*h22^7*h33^8 +
        (X*Y + X^2)*h22^7*h33^7 + (Y + 1)*h22^7*h33^6 + Y*h22^7*h33^4 +
        h22^7*h33^3 + (Y + 1)*h22^7*h33 + (X^2*Y + X)*h22^7 + h22^6*h33^9 +
        (X^2*Y + 1)*h22^6*h33^8 + (X^2*Y + X^2)*h22^6*h33^7 + (X^2*Y +
        X)*h22^6*h33^6 + X*Y*h22^6*h33^5 + X^2*h22^6*h33^4 + (X*Y +
        X^2)*h22^6*h33^3 + (X^2*Y + X^2)*h22^6*h33^2 + Y*h22^6 + h22^5*h33^10 +
        (X*Y + X^2)*h22^5*h33^9 + (X*Y + 1)*h22^5*h33^7 + h22^5*h33^5 + (X^2*Y +
        1)*h22^5*h33^4 + (Y + 1)*h22^5*h33^3 + (Y + X^2)*h22^5*h33^2 +
        X^2*Y*h22^5*h33 + X^2*h22^5 + X*h22^4*h33^11 + (X*Y + X^2)*h22^4*h33^10
        + (Y + 1)*h22^4*h33^9 + (X*Y + X^2)*h22^4*h33^5 + (X*Y + X)*h22^4*h33^4
        + (X^2*Y + X)*h22^4*h33^3 + X^2*Y*h22^4*h33^2 + (X*Y + X^2)*h22^4 +
        X*h22^3*h33^12 + (Y + X)*h22^3*h33^11 + (X^2*Y + X)*h22^3*h33^9 +
        h22^3*h33^7 + Y*h22^3*h33^3 + X*h22^3*h33^2 + (X*Y + X^2)*h22^3*h33 +
        (X*Y + X)*h22^3 + X^2*h22^2*h33^13 + (X^2*Y + 1)*h22^2*h33^12 + (Y +
        1)*h22^2*h33^11 + Y*h22^2*h33^9 + X^2*h22^2*h33^8 + (X*Y +
        X^2)*h22^2*h33^7 + (X*Y + X)*h22^2*h33^6 + X^2*Y*h22^2*h33^4 + (Y +
```

```
        X)*h22^2*h33^2 + (X*Y + X)*h22^2*h33 + (Y + X^2)*h22^2 + X^2*h22*h33^14
        + (X^2*Y + 1)*h22*h33^13 + (X^2*Y + X^2)*h22*h33^12 + (X^2*Y +
        X)*h22*h33^11 + h22*h33^9 + (X^2*Y + 1)*h22*h33^8 + (X*Y + X)*h22*h33^7
        + (X^2*Y + X)*h22*h33^6 + X^2*Y*h22*h33^5 + X*h22*h33^4 + (X*Y +
        X^2)*h22*h33^3 + (Y + 1)*h22*h33^2 + X*Y*h22 + h33^15 + (Y + X)*h33^14 +
        (X*Y + 1)*h33^12 + Y*h33^11 + h33^10 + (X*Y + X)*h33^8 + (X*Y + X)*h33^3
        + (X*Y + 1)*h33^2 + 1, 1>,
    <h22^15 + X^2*h22^14*h33 + X*Y*h22^14 + X^2*h22^13*h33^2 + Y*h22^13*h33 + (Y
        + X^2)*h22^13 + X*h22^12*h33^3 + X*Y*h22^12*h33^2 + (X*Y + X)*h22^12 +
        X*h22^11*h33^4 + (Y + X^2)*h22^11*h33^2 + (X*Y + X^2)*h22^11 +
        h22^10*h33^5 + Y*h22^10*h33^4 + (X*Y + 1)*h22^10*h33^3 + (X*Y +
        X)*h22^10*h33^2 + X^2*h22^10 + h22^9*h33^6 + X^2*Y*h22^9*h33^5 + (X*Y +
        1)*h22^9*h33^4 + (X*Y + X^2)*h22^9*h33^2 + X^2*h22^9*h33 + Y*h22^9 +
        X^2*h22^8*h33^7 + X^2*Y*h22^8*h33^6 + (X*Y + 1)*h22^8*h33^5 + (X^2*Y +
        X^2)*h22^8*h33^4 + (X*Y + X^2)*h22^8*h33^3 + h22^8*h33^2 +
        X^2*Y*h22^8*h33 + (X^2*Y + X)*h22^8 + X*h22^7*h33^8 + X^2*Y*h22^7*h33^7
        + (X^2*Y + X)*h22^7*h33^6 + (Y + X)*h22^7*h33^4 + h22^7*h33^3 + (X^2*Y +
        X)*h22^7*h33 + (Y + 1)*h22^7 + h22^6*h33^9 + X*Y*h22^6*h33^8 + (Y +
        X^2)*h22^6*h33^7 + (Y + 1)*h22^6*h33^6 + (X^2*Y + 1)*h22^6*h33^5 +
        X*h22^6*h33^4 + X^2*Y*h22^6*h33^3 + (Y + X^2)*h22^6*h33^2 + (Y +
        X)*h22^6 + h22^5*h33^10 + X^2*Y*h22^5*h33^9 + (X*Y + X)*h22^5*h33^7 +
        h22^5*h33^5 + X*Y*h22^5*h33^4 + (X^2*Y + X)*h22^5*h33^3 + (X^2*Y +
        X^2)*h22^5*h33^2 + (X*Y + X^2)*h22^5*h33 + X*h22^5 + X^2*h22^4*h33^11 +
        X^2*Y*h22^4*h33^10 + (X^2*Y + X)*h22^4*h33^9 + X^2*Y*h22^4*h33^5 + (X*Y
        + 1)*h22^4*h33^4 + (Y + 1)*h22^4*h33^3 + (X*Y + X^2)*h22^4*h33^2 +
        X^2*Y*h22^4 + X^2*h22^3*h33^12 + Y*h22^3*h33^11 + (Y + 1)*h22^3*h33^9 +
        h22^3*h33^7 + (Y + X)*h22^3*h33^3 + X^2*h22^3*h33^2 + X^2*Y*h22^3*h33 +
        (X*Y + 1)*h22^3 + X*h22^2*h33^13 + X*Y*h22^2*h33^12 + (X^2*Y +
        X)*h22^2*h33^11 + (Y + X)*h22^2*h33^9 + X*h22^2*h33^8 +
        X^2*Y*h22^2*h33^7 + (X*Y + 1)*h22^2*h33^6 + (X*Y + X^2)*h22^2*h33^4 +
        Y*h22^2*h33^2 + (X*Y + 1)*h22^2*h33 + (X^2*Y + X^2)*h22^2 + X*h22*h33^14
        + X*Y*h22*h33^13 + (Y + X^2)*h22*h33^12 + (Y + 1)*h22*h33^11 + h22*h33^9
        + X*Y*h22*h33^8 + (X*Y + 1)*h22*h33^7 + (Y + 1)*h22*h33^6 + (X*Y +
        X^2)*h22*h33^5 + X^2*h22*h33^4 + X^2*Y*h22*h33^3 + (X^2*Y + X)*h22*h33^2
        + (X^2*Y + 1)*h22 + h33^15 + Y*h33^14 + (X*Y + X)*h33^12 + (Y +
        X)*h33^11 + h33^10 + (X*Y + 1)*h33^8 + (X*Y + 1)*h33^3 + (X*Y + X)*h33^2
        + 1, 1>
]
*/
```

4. Finding uniformizer u for $x^1(1)$ and expressing variables h_{22}, h_{33} in u, variables h_1, h_2 in u and h_3.

```
/* 4_u_x1_1.txt *
/*
finding uniformizer u for the first component x1(1) of X(1)
*/
q:=2;
FX<X>:=GF(q,2);
P<Y>:=PolynomialRing(FX);
f:=Y^2 + X*Y + X^2 - X;

C<Y>:=ext<FX|f>;
```

```
Q1<h22,h33>:=PolynomialRing(C,2);
p1:=h22^15 + X*h22^14*h33 + (X^2*Y + 1)*h22^14 + X*h22^13*h33^2 + (Y +
        X)*h22^13*h33 + (X^2*Y + X^2)*h22^13 + X^2*h22^12*h33^3 + (X^2*Y +
        1)*h22^12*h33^2 + (X*Y + 1)*h22^12 + X^2*h22^11*h33^4 + (X^2*Y +
        X^2)*h22^11*h33^2 + X^2*Y*h22^11 + h22^10*h33^5 + (Y + X)*h22^10*h33^4 +
        (X*Y + X)*h22^10*h33^3 + (X*Y + 1)*h22^10*h33^2 + X*h22^10 + h22^9*h33^6
        + (X*Y + X^2)*h22^9*h33^5 + (X*Y + X)*h22^9*h33^4 + X^2*Y*h22^9*h33^2 +
        X*h22^9*h33 + (Y + X)*h22^9 + X*h22^8*h33^7 + (X*Y + X^2)*h22^8*h33^6 +
        (X*Y + X)*h22^8*h33^5 + (Y + X^2)*h22^8*h33^4 + X^2*Y*h22^8*h33^3 +
        h22^8*h33^2 + (X*Y + X^2)*h22^8*h33 + (Y + 1)*h22^8 + X^2*h22^7*h33^8 +
        (X*Y + X^2)*h22^7*h33^7 + (Y + 1)*h22^7*h33^6 + Y*h22^7*h33^4 +
        h22^7*h33^3 + (Y + 1)*h22^7*h33 + (X^2*Y + X)*h22^7 + h22^6*h33^9 +
        (X^2*Y + 1)*h22^6*h33^8 + (X^2*Y + X^2)*h22^6*h33^7 + (X^2*Y +
        X)*h22^6*h33^6 + X*Y*h22^6*h33^5 + X^2*h22^6*h33^4 + (X*Y +
        X^2)*h22^6*h33^3 + (X^2*Y + X^2)*h22^6*h33^2 + Y*h22^6 + h22^5*h33^10 +
        (X*Y + X^2)*h22^5*h33^9 + (X*Y + 1)*h22^5*h33^7 + h22^5*h33^5 + (X^2*Y +
        1)*h22^5*h33^4 + (Y + 1)*h22^5*h33^3 + (Y + X^2)*h22^5*h33^2 +
        X^2*Y*h22^5*h33 + X^2*h22^5 + X*h22^4*h33^11 + (X*Y + X^2)*h22^4*h33^10
        + (Y + 1)*h22^4*h33^9 + (X*Y + X^2)*h22^4*h33^5 + (X*Y + X)*h22^4*h33^4
        + (X^2*Y + X)*h22^4*h33^3 + X^2*Y*h22^4*h33^2 + (X*Y + X^2)*h22^4 +
        X*h22^3*h33^12 + (Y + X)*h22^3*h33^11 + (X^2*Y + X)*h22^3*h33^9 +
        h22^3*h33^7 + Y*h22^3*h33^3 + X*h22^3*h33^2 + (X*Y + X^2)*h22^3*h33 +
        (X*Y + X)*h22^3 + X^2*h22^2*h33^13 + (X^2*Y + 1)*h22^2*h33^12 + (Y +
        1)*h22^2*h33^11 + Y*h22^2*h33^9 + X^2*h22^2*h33^8 + (X*Y +
        X^2)*h22^2*h33^7 + (X*Y + X)*h22^2*h33^6 + X^2*Y*h22^2*h33^4 + (Y +
        X)*h22^2*h33^2 + (X*Y + X)*h22^2*h33 + (Y + X^2)*h22^2 + X^2*h22*h33^14
        + (X^2*Y + 1)*h22*h33^13 + (X^2*Y + X^2)*h22*h33^12 + (X^2*Y +
        X)*h22*h33^11 + h22*h33^9 + (X^2*Y + 1)*h22*h33^8 + (X*Y + X)*h22*h33^7
        + (X^2*Y + X)*h22*h33^6 + X^2*Y*h22*h33^5 + X*h22*h33^4 + (X*Y +
        X^2)*h22*h33^3 + (Y + 1)*h22*h33^2 + X*Y*h22 + h33^15 + (Y + X)*h33^14 +
        (X*Y + 1)*h33^12 + Y*h33^11 + h33^10 + (X*Y + X)*h33^8 + (X*Y + X)*h33^3
        + (X*Y + 1)*h33^2 + 1;
F<h22,h33>:=FunctionField(p1);
/*
Genus(F) = 0, moreover, F is rational
Let's pick one rational place to compute a uniformizer using RiemannRochSpace
*/

P:=InfinitePlaces(F);
/*
[ (1/h33, (X^2*Y*h22^14 + X*Y*h22^12*h33^2 + h22^12*h33 + X*h22^11*h33^2 +
    X*Y*h22^10*h33^4 + X*h22^10*h33^3 + h22^10*h33^2 + h22^9*h33^4 +
    Y*h22^8*h33^6 + X^2*h22^8*h33^4 + X*h22^7*h33^6 + X*Y*h22^6*h33^8 +
    h22^6*h33^7 + X*h22^5*h33^8 + Y*h22^4*h33^10 + X^2*h22^4*h33^9 +
    X^2*h22^3*h33^10 + Y*h22^2*h33^12 + X*h22^2*h33^11 + X^2*h22^2*h33^10 +
    h22*h33^12 + X^2*Y*h33^14 + X^2*h33^12)/h33^12), (1/h33, ((Y + X^2)*h22^14 +
    (X*Y + 1)*h22^13*h33 + Y*h22^12*h33 + X^2*Y*h22^11*h33^2 + (X^2*Y +
    X)*h22^10*h33^4 + X^2*Y*h22^10*h33^3 + h22^10*h33^2 + (Y + X^2)*h22^9*h33^5
    + X^2*Y*h22^9*h33^4 + Y*h22^8*h33^5 + X^2*h22^8*h33^4 + X^2*Y*h22^7*h33^6 +
    (X^2*Y + X)*h22^6*h33^8 + (Y + X^2)*h22^5*h33^9 + X*Y*h22^5*h33^8 +
    Y*h22^3*h33^10 + (X*Y + 1)*h22^2*h33^12 + X^2*h22^2*h33^10 + (X^2*Y +
    X)*h22*h33^13 + X^2*Y*h22*h33^12 + Y*h33^13 + X^2*h33^12)/h33^12) ]

Degree(P[1]) = 1
*/
```

```
V,h:=RiemannRochSpace(P[1]);
u:=h(Basis(V)[2]);

Write("u_inf.txt",u);

/*
express h33 in u
*/
q:=2;
FX<X>:=GF(q,2);
P<Y>:=PolynomialRing(FX);
f:=Y^2 + X*Y + X^2 - X;

C<Y>:=ext<FX|f>;
K<h33>:=RationalFunctionField(C);
P<h22>:=PolynomialRing(K);

p1:=h22^15 + X*h22^14*h33 + (X^2*Y + 1)*h22^14 + X*h22^13*h33^2 + (Y +
        X)*h22^13*h33 + (X^2*Y + X^2)*h22^13 + X^2*h22^12*h33^3 + (X^2*Y +
        1)*h22^12*h33^2 + (X*Y + 1)*h22^12 + X^2*h22^11*h33^4 + (X^2*Y +
        X^2)*h22^11*h33^2 + X^2*Y*h22^11 + h22^10*h33^5 + (Y + X)*h22^10*h33^4 +
        (X*Y + X)*h22^10*h33^3 + (X*Y + 1)*h22^10*h33^2 + X*h22^10 + h22^9*h33^6
        + (X*Y + X^2)*h22^9*h33^5 + (X*Y + X)*h22^9*h33^4 + X^2*Y*h22^9*h33^2 +
        X*h22^9*h33 + (Y + X)*h22^9 + X*h22^8*h33^7 + (X*Y + X^2)*h22^8*h33^6 +
        (X*Y + X)*h22^8*h33^5 + (Y + X^2)*h22^8*h33^4 + X^2*Y*h22^8*h33^3 +
        h22^8*h33^2 + (X*Y + X^2)*h22^8*h33 + (Y + 1)*h22^8 + X^2*h22^7*h33^8 +
        (X*Y + X^2)*h22^7*h33^7 + (Y + 1)*h22^7*h33^6 + Y*h22^7*h33^4 +
        h22^7*h33^3 + (Y + 1)*h22^7*h33 + (X^2*Y + X)*h22^7 + h22^6*h33^9 +
        (X^2*Y + 1)*h22^6*h33^8 + (X^2*Y + X^2)*h22^6*h33^7 + (X^2*Y +
        X)*h22^6*h33^6 + X*Y*h22^6*h33^5 + X^2*h22^6*h33^4 + (X*Y +
        X^2)*h22^6*h33^3 + (X^2*Y + X^2)*h22^6*h33^2 + Y*h22^6 + h22^5*h33^10 +
        (X*Y + X^2)*h22^5*h33^9 + (X*Y + 1)*h22^5*h33^7 + h22^5*h33^5 + (X^2*Y +
        1)*h22^5*h33^4 + (Y + 1)*h22^5*h33^3 + (Y + X^2)*h22^5*h33^2 +
        X^2*Y*h22^5*h33 + X^2*h22^5 + X*h22^4*h33^11 + (X*Y + X^2)*h22^4*h33^10
        + (Y + 1)*h22^4*h33^9 + (X*Y + X^2)*h22^4*h33^5 + (X*Y + X)*h22^4*h33^4
        + (X^2*Y + X)*h22^4*h33^3 + X^2*Y*h22^4*h33^2 + (X*Y + X^2)*h22^4 +
        X*h22^3*h33^12 + (Y + X)*h22^3*h33^11 + (X^2*Y + X)*h22^3*h33^9 +
        h22^3*h33^7 + Y*h22^3*h33^3 + X*h22^3*h33^2 + (X*Y + X^2)*h22^3*h33 +
        (X*Y + X)*h22^3 + X^2*h22^2*h33^13 + (X^2*Y + 1)*h22^2*h33^12 + (Y +
        1)*h22^2*h33^11 + Y*h22^2*h33^9 + X^2*h22^2*h33^8 + (X*Y +
        X^2)*h22^2*h33^7 + (X*Y + X)*h22^2*h33^6 + X^2*Y*h22^2*h33^4 + (Y +
        X)*h22^2*h33^2 + (X*Y + X)*h22^2*h33 + (Y + X^2)*h22^2 + X^2*h22*h33^14
        + (X^2*Y + 1)*h22*h33^13 + (X^2*Y + X^2)*h22*h33^12 + (X^2*Y +
        X)*h22*h33^11 + h22*h33^9 + (X^2*Y + 1)*h22*h33^8 + (X*Y + X)*h22*h33^7
        + (X^2*Y + X)*h22*h33^6 + X^2*Y*h22*h33^5 + X*h22*h33^4 + (X*Y +
        X^2)*h22*h33^3 + (Y + 1)*h22*h33^2 + X*Y*h22 + h33^15 + (Y + X)*h33^14 +
        (X*Y + 1)*h33^12 + Y*h33^11 + h33^10 + (X*Y + X)*h33^8 + (X*Y + X)*h33^3
        + (X*Y + 1)*h33^2 + 1;

F<h22>:=FunctionField(p1);

load "u_inf.txt";
mh:=MinimalPolynomial(u,K);
```

```
mh;
/*
h22^15 + Y*h22^14 + (X*Y + 1)*h22^13 + (X*Y + X)*h22^12 + (Y + X)*h22^11 +
    h22^10 + ((X^2*Y + X)*h33 + Y)*h22^9 + ((Y + 1)*h33 + (X*Y + 1))*h22^8 +
    (X*Y + X)*h22^7 + (Y + X)*h22^6 + h22^5 + Y*h22^4 + (X*Y + 1)*h22^3 + (X*Y +
    X)*h22^2 + (h33 + (Y + X))*h22 + X*Y*h33 + 1

It is a polynomial in C(h33)[h22]. Rename the variable h22 by u and solve
this polynomial for variable h33

mh:=u^15 + Y*u^14 + (X*Y + 1)*u^13 + (X*Y + X)*u^12 + (Y + X)*u^11 +
    u^10 + ((X^2*Y + X)*h33 + Y)*u^9 + ((Y + 1)*h33 + (X*Y + 1))*u^8 +
    (X*Y + X)*u^7 + (Y + X)*u^6 + u^5 + Y*u^4 + (X*Y + 1)*u^3 + (X*Y +
    X)*u^2 + (h33 + (Y + X))*u + X*Y*h33 + 1;
solve(mh,h33) mod 2; //in Maple

h33:=(X*Y*u^13 + Y*u^14 + u^15 + X*Y*u^12 + X*u^12 + u^13 + X*u^11 + Y*u^11
    + X*Y*u^8 + Y*u^9 + u^10 + X*Y*u^7 + X*u^7 + u^8 + X*u^6 + Y*u^6 + X*Y*u^3
    + Y*u^4 + u^5 + X*Y*u^2 + X*u^2 + u^3 + X*u + Y*u + 1)/(X^2*Y*u^9 + X*u^9
    + Y*u^8 + u^8 + X*Y + u);
*/

/*
express h22 in u
*/

q:=2;
FX<X>:=GF(q,2);
P<Y>:=PolynomialRing(FX);
f:=Y^2 + X*Y + X^2 - X;

C<Y>:=ext<FX|f>;
K<h22>:=RationalFunctionField(C);
P<h33>:=PolynomialRing(K);

p1:=h22^15 + X*h22^14*h33 + (X^2*Y + 1)*h22^14 + X*h22^13*h33^2 + (Y +
        X)*h22^13*h33 + (X^2*Y + X^2)*h22^13 + X^2*h22^12*h33^3 + (X^2*Y +
        1)*h22^12*h33^2 + (X*Y + 1)*h22^12 + X^2*h22^11*h33^4 + (X^2*Y +
        X^2)*h22^11*h33^2 + X^2*Y*h22^11 + h22^10*h33^5 + (Y + X)*h22^10*h33^4 +
        (X*Y + X)*h22^10*h33^3 + (X*Y + 1)*h22^10*h33^2 + X*h22^10 + h22^9*h33^6
        + (X*Y + X^2)*h22^9*h33^5 + (X*Y + X)*h22^9*h33^4 + X^2*Y*h22^9*h33^2 +
        X*h22^9*h33 + (Y + X)*h22^9 + X*h22^8*h33^7 + (X*Y + X^2)*h22^8*h33^6 +
        (X*Y + X)*h22^8*h33^5 + (Y + X^2)*h22^8*h33^4 + X^2*Y*h22^8*h33^3 +
        h22^8*h33^2 + (X*Y + X^2)*h22^8*h33 + (Y + 1)*h22^8 + X^2*h22^7*h33^8 +
        (X*Y + X^2)*h22^7*h33^7 + (Y + 1)*h22^7*h33^6 + Y*h22^7*h33^4 +
        h22^7*h33^3 + (Y + 1)*h22^7*h33 + (X^2*Y + X)*h22^7 + h22^6*h33^9 +
        (X^2*Y + 1)*h22^6*h33^8 + (X^2*Y + X^2)*h22^6*h33^7 + (X^2*Y +
        X)*h22^6*h33^6 + X*Y*h22^6*h33^5 + X^2*h22^6*h33^4 + (X*Y +
        X^2)*h22^6*h33^3 + (X^2*Y + X^2)*h22^6*h33^2 + Y*h22^6 + h22^5*h33^10 +
        (X*Y + X^2)*h22^5*h33^9 + (X*Y + 1)*h22^5*h33^7 + h22^5*h33^5 + (X^2*Y +
        1)*h22^5*h33^4 + (Y + 1)*h22^5*h33^3 + (Y + X^2)*h22^5*h33^2 +
        X^2*Y*h22^5*h33 + X^2*h22^5 + X*h22^4*h33^11 + (X*Y + X^2)*h22^4*h33^10
        + (Y + 1)*h22^4*h33^9 + (X*Y + X^2)*h22^4*h33^5 + (X*Y + X)*h22^4*h33^4
        + (X^2*Y + X)*h22^4*h33^3 + X^2*Y*h22^4*h33^2 + (X*Y + X^2)*h22^4 +
        X*h22^3*h33^12 + (Y + X)*h22^3*h33^11 + (X^2*Y + X)*h22^3*h33^9 +
```

```
        h22^3*h33^7 + Y*h22^3*h33^3 + X*h22^3*h33^2 + (X*Y + X^2)*h22^3*h33 +
        (X*Y + X)*h22^3 + X^2*h22^2*h33^13 + (X^2*Y + 1)*h22^2*h33^12 + (Y +
        1)*h22^2*h33^11 + Y*h22^2*h33^9 + X^2*h22^2*h33^8 + (X*Y +
        X^2)*h22^2*h33^7 + (X*Y + X)*h22^2*h33^6 + X^2*Y*h22^2*h33^4 + (Y +
        X)*h22^2*h33^2 + (X*Y + X)*h22^2*h33 + (Y + X^2)*h22^2 + X^2*h22*h33^14
        + (X^2*Y + 1)*h22*h33^13 + (X^2*Y + X^2)*h22*h33^12 + (X^2*Y +
        X)*h22*h33^11 + h22*h33^9 + (X^2*Y + 1)*h22*h33^8 + (X*Y + X)*h22*h33^7
        + (X^2*Y + X)*h22*h33^6 + X^2*Y*h22*h33^5 + X*h22*h33^4 + (X*Y +
        X^2)*h22*h33^3 + (Y + 1)*h22*h33^2 + X*Y*h22 + h33^15 + (Y + X)*h33^14 +
        (X*Y + 1)*h33^12 + Y*h33^11 + h33^10 + (X*Y + X)*h33^8 + (X*Y + X)*h33^3
        + (X*Y + 1)*h33^2 + 1;
F<h33>:=FunctionField(p1);

load "u_inf.txt";
mh2:=MinimalPolynomial(u,K);
mh2;
/*
h33^15 + Y*h33^14 + (X*Y + 1)*h33^13 + (X^2*Y + X^2)*h33^12 + (Y + X)*h33^11 +
    h33^10 + ((Y + X^2)*h22 + Y)*h33^9 + ((X*Y + X)*h22 + (X^2*Y + X))*h33^8 +
    (X*Y + X)*h33^7 + (Y + X)*h33^6 + h33^5 + X*Y*h33^4 + (X^2*Y + X)*h33^3 +
    (X^2*Y + X^2)*h33^2 + (X*h22 + (X*Y + X^2))*h33 + X^2*Y*h22 + X^2



It is a polynomial in C(h22)[h33]. Rename the variable h33 by u and solve
this polynomial for variable h22


mh2:=u^15 + Y*u^14 + (X*Y + 1)*u^13 + (X^2*Y + X^2)*u^12 + (Y + X)*u^11 +
    u^10 + ((Y + X^2)*h22 + Y)*u^9 + ((X*Y + X)*h22 + (X^2*Y + X))*u^8 +
    (X*Y + X)*u^7 + (Y + X)*u^6 + u^5 + X*Y*u^4 + (X^2*Y + X)*u^3 +
    (X^2*Y + X^2)*u^2 + (X*h22 + (X*Y + X^2))*u + X^2*Y*h22 + X^2;


solve(mh2,h22) mod 2; //in Maple

we get
h22 := (X^2*Y*u^12 + X*Y*u^13 + Y*u^14 + u^15 + X^2*u^12 + u^13 + X*u^11 + Y*u^11
    + X^2*Y*u^8 + Y*u^9 + u^10 + X*Y*u^7 + X*u^8 + X*u^7 + X*u^6 + Y*u^6
    + X^2*Y*u^3 + X*Y*u^4 + X^2*Y*u^2 + u^5 + X^2*u^2 + X*u^3 + X^2*u + X*Y*u
    + X^2)/(X^2*u^9 + X*Y*u^8 + Y*u^9 + X*u^8 + X^2*Y + X*u)
*/


/*
express other variables in u
*/
q:=2;
FX<X>:=GF(q,2);
P<Y>:=PolynomialRing(FX);
f:=Y^2 + X*Y + X^2 - X;

C<Y>:=ext<FX|f>;

K<u>:=RationalFunctionField(C);
```

```
/*
F(h22,h33)=F(u)
*/

h33:=(X*Y*u^13 + Y*u^14 + u^15 + X*Y*u^12 + X*u^12 + u^13 + X*u^11 + Y*u^11
    + X*Y*u^8 + Y*u^9 + u^10 + X*Y*u^7 + X*u^7 + u^8 + X*u^6 + Y*u^6 + X*Y*u^3
    + Y*u^4 + u^5 + X*Y*u^2 + X*u^2 + u^3 + X*u + Y*u + 1)/(X^2*Y*u^9 + X*u^9
    + Y*u^8 + u^8 + X*Y + u);

h22 := (X^2*Y*u^12 + X*Y*u^13 + Y*u^14 + u^15 + X^2*u^12 + u^13 + X*u^11 + Y*u^11
    + X^2*Y*u^8 + Y*u^9 + u^10 + X*Y*u^7 + X*u^8 + X*u^7 + X*u^6 + Y*u^6
    + X^2*Y*u^3 + X*Y*u^4 + X^2*Y*u^2 + u^5 + X^2*u^2 + X*u^3 + X^2*u + X*Y*u
    + X^2)/(X^2*u^9 + X*Y*u^8 + Y*u^9 + X*u^8 + X^2*Y + X*u);

P3<h3>:=PolynomialRing(K);

F3<h3>:=ext<K|h3^((q^2+1)*(q+1))-h33>;
/*
Degree(F3); =15
this shows that h2 should be in F(u,h3).
*/
P2<h2>:=PolynomialRing(F3);
poly1:=Factorization(h2^(q^2+1)-h22);
/*
[
    <h2 + ((X^2*Y + X^2)*u^3 + (X*Y + X^2)*u^2 + X*u + X^2*Y)/(u^3 + Y*u^2 +
        (X*Y + 1)*u + (X*Y + X))*h3^3, 1>,
    <h2 + (X*u^3 + X*Y*u^2 + (X^2*Y + X)*u + (Y + 1))/(u^3 + Y*u^2 + (X*Y + 1)*u
        + (X*Y + X))*h3^3, 1>,
    <h2 + ((X^2*Y + X)*u^3 + (X^2*Y + X^2)*u^2 + (X*Y + X^2)*u + X^2)/(u^3 +
        Y*u^2 + (X*Y + 1)*u + (X*Y + X))*h3^3, 1>,
    <h2 + ((X*Y + X^2)*u^3 + X*u^2 + X*Y*u + (Y + X^2))/(u^3 + Y*u^2 + (X*Y +
        1)*u + (X*Y + X))*h3^3, 1>,
    <h2 + (X*Y*u^3 + (X^2*Y + X)*u^2 + (X^2*Y + X^2)*u + (X^2*Y + 1))/(u^3 +
        Y*u^2 + (X*Y + 1)*u + (X*Y + X))*h3^3, 1>
]
this shows that h2 is infact in F(u,h3).
*/
/*
using p(h2,h3) to check which factor is the right one
*/
h2:=((X^2*Y + X^2)*u^3 + (X*Y + X^2)*u^2 + X*u + X^2*Y)/(u^3 + Y*u^2 +
        (X*Y + 1)*u + (X*Y + X))*h3^3;
h2^30 + (X*Y + X)*h2^29*h3^3 + (Y + X)*h2^27*h3^9 + (X*Y + 1)*h2^26*h3^12 +
        (Y + 1)*h2^25 + (X*Y + X)*h2^24*h3^18 + (X^2*Y + X^2)*h2^24*h3^3 +
        Y*h2^23*h3^21 + (X^2*Y + 1)*h2^23*h3^6 + X^2*Y*h2^22*h3^9 + (X*Y +
        1)*h2^21*h3^27 + (X^2*Y + X)*h2^21*h3^12 + h2^20*h3^30 + (Y +
        1)*h2^20*h3^15 + (X*Y + 1)*h2^20 + (X^2*Y + X^2)*h2^19*h3^18 +
        Y*h2^18*h3^36 + (X*Y + X)*h2^18*h3^6 + (Y + X)*h2^17*h3^39 + (Y +
        X^2)*h2^17*h3^24 + X*h2^17*h3^9 + (X^2*Y + 1)*h2^16*h3^27 +
        X*Y*h2^16*h3^12 + h2^15*h3^45 + (Y + 1)*h2^15*h3^30 + X*Y*h2^15*h3^15 +
        (Y + X)*h2^15 + (X^2*Y + X^2)*h2^14*h3^33 + (Y + 1)*h2^14*h3^18 +
        h2^14*h3^3 + Y*h2^13*h3^51 + X*Y*h2^13*h3^36 + X*h2^13*h3^21 + (X*Y +
        X)*h2^13*h3^6 + (Y + X)*h2^12*h3^54 + X^2*Y*h2^12*h3^39 + (X^2*Y +
        X)*h2^12*h3^9 + (X^2*Y + X)*h2^11*h3^42 + (Y + X^2)*h2^11*h3^27 +
```

```
        X*h2^11*h3^12 + h2^10*h3^60 + (Y + X^2)*h2^10*h3^45 + X*h2^10*h3^30 + (Y
        + X)*h2^10*h3^15 + (X*Y + 1)*h2^10 + (X*Y + X)*h2^9*h3^63 +
        X^2*Y*h2^9*h3^48 + (X*Y + X)*h2^9*h3^33 + (X*Y + 1)*h2^9*h3^18 + (X*Y +
        X)*h2^9*h3^3 + X*Y*h2^8*h3^51 + (X^2*Y + X)*h2^8*h3^36 + (X*Y +
        X)*h2^8*h3^21 + (Y + X)*h2^8*h3^6 + (Y + X)*h2^7*h3^69 + (Y +
        X^2)*h2^7*h3^54 + (X^2*Y + 1)*h2^7*h3^39 + (X*Y + 1)*h2^7*h3^24 +
        X*h2^7*h3^9 + (X*Y + 1)*h2^6*h3^72 + X*Y*h2^6*h3^42 + (X*Y +
        1)*h2^6*h3^27 + (Y + X^2)*h2^6*h3^12 + X*h2^5*h3^60 + (X*Y +
        1)*h2^5*h3^45 + h2^5*h3^30 + (X*Y + X^2)*h2^5*h3^15 + (Y + 1)*h2^5 +
        (X*Y + X)*h2^4*h3^78 + Y*h2^4*h3^48 + (X^2*Y + X)*h2^4*h3^33 + (X*Y +
        X)*h2^4*h3^18 + X^2*h2^4*h3^3 + Y*h2^3*h3^81 + X*Y*h2^3*h3^66 +
        X*h2^3*h3^51 + (X^2*Y + X^2)*h2^3*h3^36 + X*Y*h2^3*h3^21 + (X*Y +
        X^2)*h2^2*h3^69 + (Y + X)*h2^2*h3^54 + (Y + 1)*h2^2*h3^39 + (Y +
        X)*h2^2*h3^24 + (Y + X^2)*h2^2*h3^9 + (X*Y + 1)*h2*h3^87 + h2*h3^57 +
        X^2*Y*h2*h3^42 + (X^2*Y + X^2)*h2*h3^27 + (X^2*Y + 1)*h2*h3^12 + h3^90 +
        X*h3^75 + h3^60 + X^2*h3^45 + X^2*h3^30 + 1;
/*
=0. OK. The other factors do not give zero.
*/

F2<h2>:=ext<F3|h2 + ((X^2*Y + X^2)*u^3 + (X*Y + X^2)*u^2 + X*u + X^2*Y)/(u^3
    + Y*u^2 + (X*Y + 1)*u + (X*Y + X))*h3^3>;
P1<h1>:=PolynomialRing(F2);
/*
to find the expression of h1 in h2,h3 we can pick any relations between h1,h2,h3
from relations L1 or L2 in 1_normalize.mag when defining Drinfeld modules
*/
Factorization((Y + X^2)*h1^4*h2 + (Y + 1)*h1^4*h3^3 + (X*Y + 1)*h1^2*h3^17 + (Y +
        1)*h1*h2^8 + X^2*Y*h1*h3^24 + (X*Y + X^2)*h2^10*h3 + (X^2*Y +
        1)*h2^9*h3^4 + X^2*Y*h2^8*h3^7 + Y*h2^5*h3^16 + X*Y*h2^4*h3^19 + (X*Y +
        X)*h2^2*h3^25 + X^2*h2*h3^28 + (X^2*Y + 1)*h3^31 + (X^2*Y + X^2)*h3^16 +
        X^2*h3);
/*
[
    <h1 + (X*Y*u^4 + (X*Y + 1)*u + X^2*Y)/(u^7 + Y*u^6 + (X*Y + 1)*u^5 + (X*Y +
        X)*u^4 + (Y + X)*u^3 + u^2 + Y*u + (X*Y + 1))*h3^7, 1>,
    <h1^3 + (X*Y*u^4 + (X*Y + 1)*u + X^2*Y)/(u^7 + Y*u^6 + (X*Y + 1)*u^5 + (X*Y
        + X)*u^4 + (Y + X)*u^3 + u^2 + Y*u + (X*Y + 1))*h3^7*h1^2 + (Y*u^17 +
        (X*Y + 1)*u^16 + (Y + X^2)*u^11 + (Y + 1)*u^10 + (X^2*Y + 1)*u^9 +
        X*Y*u^8 + (Y + X)*u^5 + u^4 + (X*Y + X)*u^3 + (X*Y + X)*u^2 + X*u +
        (X^2*Y + X))/(u^17 + Y*u^16 + (Y + X^2)*u^14 + (X^2*Y + 1)*u^12 +
        X^2*Y*u^10 + (Y + 1)*u^8 + X^2*u^6 + (Y + X^2)*u^4 + (X^2*Y + 1)*u^2 +
        Y*u + (Y + 1))*h3^14*h1 + ((X*Y + 1)*u^23 + (X*Y + X)*u^22 + (Y +
        X)*u^21 + Y*u^19 + (X*Y + 1)*u^18 + (Y + X)*u^17 + Y*u^16 + X^2*Y*u^14 +
        (Y + 1)*u^12 + u^11 + (X^2*Y + X^2)*u^10 + (X*Y + 1)*u^9 + (X^2*Y +
        X)*u^8 + (X*Y + 1)*u^6 + (X^2*Y + X)*u^5 + X*Y*u^4 + X*Y*u^3 + (Y +
        1)*u^2 + X*u + X^2*Y)/(u^17 + X*Y*u^16 + (Y + X^2)*u^14 + (X^2*Y +
        X^2)*u^13 + (Y + X)*u^12 + X^2*Y*u^10 + u^9 + (Y + X^2)*u^8 + X*u^6 +
        Y*u^5 + (Y + X^2)*u^4 + (X*Y + X^2)*u^2 + (X^2*Y + 1)*u + (Y + 1))*h3^6,
    1>
]
*/
```

```
h1 := (X*Y*u^4 + (X*Y + 1)*u + X^2*Y)/(u^7 + Y*u^6 + (X*Y + 1)*u^5 + (X*Y +
        X)*u^4 + (Y + X)*u^3 + u^2 + Y*u + (X*Y + 1))*h3^7;
g3 := X*Y*h3;
g2 := (X*Y + X)*h3^3;
g1 := (Y + 1)*h1 + (Y + X)*h2^2*h3 + (X*Y + 1)*h2*h3^4 + h3^7;
g0 := (X^2*Y + 1)*h1^2*h3 + (X*Y + X)*h1*h3^8 + (X^2*Y + X)*h2^5 + (X^2*Y +
        X)*h2^4*h3^3 + (X*Y + 1)*h2^2*h3^9 + X*h2*h3^12 + Y*h3^15 + Y + X^2;
/*
g0 = X^2
*/
/*
check relations L1, L2
*/
    g3 + X*Y*h3,
    g2 + (X*Y + X)*h3^3,
    g1 + (Y + 1)*h1 + (Y + X)*h2^2*h3 + (X*Y + 1)*h2*h3^4 + h3^7,
    g0 + (X^2*Y + 1)*h1^2*h3 + (X*Y + X)*h1*h3^8 + (X^2*Y + X)*h2^5 + (X^2*Y +
        X)*h2^4*h3^3 + (X*Y + 1)*h2^2*h3^9 + X*h2*h3^12 + Y*h3^15 + Y + X^2,
    h1^4*h2 + Y*h1^4*h3^3 + X*h1^2*h3^17 + Y*h1*h2^8 + (Y + X)*h1*h3^24 + (Y +
        X^2)*h2^10*h3 + (X*Y + 1)*h2^9*h3^4 + (Y + X)*h2^8*h3^7 + (X*Y +
        X^2)*h2^5*h3^16 + (X^2*Y + 1)*h2^4*h3^19 + X*Y*h2^2*h3^25 + (X*Y +
        X)*h2*h3^28 + (X*Y + 1)*h3^31 + X^2*Y*h3^16 + (X*Y + X)*h3,
    (X^2*Y + 1)*h1^9 + (X*Y + 1)*h1^8*h2^2*h3 + h1^8*h2*h3^4 + (Y +
        X^2)*h1^8*h3^7 + h1^4*h3^35 + (X^2*Y + 1)*h1^2*h2^16*h3 + (Y +
        X^2)*h1^2*h3^49 + (X*Y + 1)*h1*h2^16*h3^8 + (X^2*Y + 1)*h1*h2^8*h3^32 +
        h1*h3^56 + (X^2*Y + X)*h2^21 + (Y + X)*h2^20*h3^3 + (X^2*Y +
        1)*h2^18*h3^9 + Y*h2^17*h3^12 + (Y + 1)*h2^16*h3^15 + (Y + X)*h2^16 +
        h2^10*h3^33 + (X*Y + X)*h2^9*h3^36 + X*h2^5*h3^48 + (X^2*Y +
        1)*h2^4*h3^51 + (Y + X^2)*h2^2*h3^57 + (Y + X)*h2*h3^60 + h2 + (X^2*Y +
        X)*h3^63 + X^2*h3^48 + (Y + X)*h3^3,
    X^2*h1^18*h3 + (Y + X^2)*h1^17*h3^8 + (X^2*Y + X^2)*h1^16*h2^5 + (X^2*Y +
        X^2)*h1^16*h2^4*h3^3 + X*h1^16*h2^2*h3^9 + X^2*h1^16*h2*h3^12 + (Y +
        X^2)*h1^16*h3^15 + Y*h1^16 + (Y + X^2)*h1^9*h3^64 + (X*Y +
        X)*h1^8*h2^2*h3^65 + Y*h1^8*h2*h3^68 + (Y + X)*h1^8*h3^71 + (Y +
        1)*h1^2*h2^32*h3^17 + X^2*Y*h1^2*h2^16*h3^65 + (X^2*Y + 1)*h1^2*h3^113 +
        (X*Y + X^2)*h1*h2^40 + X*h1*h2^32*h3^24 + X^2*Y*h1*h2^16*h3^72 + (X^2*Y
        + X^2)*h1*h2^8*h3^96 + (Y + X)*h1*h3^120 + X*h1 + X^2*h2^42*h3 + (Y +
        1)*h2^41*h3^4 + X^2*Y*h2^40*h3^7 + X*Y*h2^37*h3^16 + X*Y*h2^36*h3^19 +
        (Y + X^2)*h2^34*h3^25 + (X^2*Y + X)*h2^33*h3^28 + (X^2*Y +
        1)*h2^32*h3^31 + X^2*Y*h2^32*h3^16 + (X*Y + X^2)*h2^21*h3^64 + (X*Y +
        X^2)*h2^20*h3^67 + (Y + X^2)*h2^18*h3^73 + Y*h2^17*h3^76 + (X^2*Y +
        X)*h2^16*h3^79 + (X^2*Y + 1)*h2^16*h3^64 + (X^2*Y + 1)*h2^10*h3^97 + (Y
        + X^2)*h2^9*h3^100 + X^2*h2^8*h3^103 + (X^2*Y + X)*h2^5*h3^112 + (X^2*Y
        + X)*h2^4*h3^115 + Y*h2^2*h3 + X^2*h2*h3^124 + (Y + X)*h2*h3^4 + (X^2*Y
        + X)*h3^127 + (Y + X^2)*h3^112 + (X*Y + 1)*h3^7,
    (Y + X^2)*h1^4*h2 + (Y + 1)*h1^4*h3^3 + (X*Y + 1)*h1^2*h3^17 + (Y +
        1)*h1*h2^8 + X^2*Y*h1*h3^24 + (X*Y + X^2)*h2^10*h3 + (X^2*Y +
        1)*h2^9*h3^4 + X^2*Y*h2^8*h3^7 + Y*h2^5*h3^16 + X*Y*h2^4*h3^19 + (X*Y +
        X)*h2^2*h3^25 + X^2*h2*h3^28 + (X^2*Y + 1)*h3^31 + (X^2*Y + X^2)*h3^16 +
        X^2*h3,
    (X^2*Y + X)*h1^9 + (Y + X)*h1^8*h2^2*h3 + (Y + 1)*h1^8*h2*h3^4 + h1^8*h3^7 +
        (X*Y + 1)*h1^4*h2*h3^32 + (X^2*Y + 1)*h1^2*h2^16*h3 + X^2*h1*h2^16*h3^8
        + Y*h1*h2^8*h3^32 + h1*h3^56 + h2^21 + (X^2*Y + X)*h2^20*h3^3 + (X*Y +
        1)*h2^18*h3^9 + (X^2*Y + 1)*h2^17*h3^12 + Y*h2^16*h3^15 + (Y +
```

```
        X^2)*h2^16 + (X*Y + X)*h2^9*h3^36 + X*h2^5*h3^48 + (Y + X)*h2*h3^60 + (Y
        + 1)*h2 + (X*Y + X)*h3^48 + (X*Y + X)*h3^3,
    (X^2*Y + 1)*h1^18*h3 + Y*h1^17*h3^8 + (X^2*Y + X)*h1^16*h2^5 + (X^2*Y +
        X)*h1^16*h2^4*h3^3 + (X*Y + 1)*h1^16*h2^2*h3^9 + X*h1^16*h2*h3^12 +
        Y*h1^16*h3^15 + X*h1^16 + (Y + X)*h1^9*h3^64 + X^2*Y*h1*h2^40 +
        X^2*Y*h1*h2^32*h3^24 + Y*h1*h2^16*h3^72 + X^2*h1*h2^8*h3^96 + (X*Y +
        X)*h1*h3^120 + (X^2*Y + 1)*h1 + (Y + X)*h2^32*h3^16 + (X*Y +
        1)*h2^16*h3^64 + (Y + X)*h2^2*h3 + (X*Y + 1)*h2*h3^4 + h3^112 + h3^7,
    (X^2*Y + X^2)*h1^4*h3^2 + Y*h1^2*h3^16 + (X^2*Y + 1)*h1^2*h3 + (X*Y +
        X)*h1*h3^8 + (X^2*Y + 1)*h2^10 + (X^2*Y + 1)*h2^8*h3^6 + (X^2*Y +
        X)*h2^5 + (Y + X)*h2^4*h3^18 + (X^2*Y + X)*h2^4*h3^3 + X^2*h2^2*h3^24 +
        (X*Y + 1)*h2^2*h3^9 + X*h2*h3^12 + (X*Y + 1)*h3^30 + Y*h3^15 + X^2*Y + 1;
/*
all are 0. OK
*/
```

The same procedure applies for finding the uniformizer v for $x^2(1)$ and for variable substitutions by replacing component p^1 by p^2 and variables in h's by t's.

5. Expressing elements in Figure 4.4.

```
/* 5_rewrite_D_modules.txt */
q:=2;
FX<X>:=GF(q,2);
P<Y>:=PolynomialRing(FX);
f:=Y^2 + X*Y + X^2 - X;

C<Y>:=ext<FX|f>;

K<u>:=RationalFunctionField(C);
/*
F(h22,h33)=F(u)
*/

h33:=(X*Y*u^13 + Y*u^14 + u^15 + X*Y*u^12 + X*u^12 + u^13 + X*u^11 + Y*u^11
    + X*Y*u^8 + Y*u^9 + u^10 + X*Y*u^7 + X*u^7 + u^8 + X*u^6 + Y*u^6 + X*Y*u^3
    + Y*u^4 + u^5 + X*Y*u^2 + X*u^2 + u^3 + X*u + Y*u + 1)/(X^2*Y*u^9 + X*u^9
    + Y*u^8 + u^8 + X*Y + u);

h22 := (X^2*Y*u^12 + X*Y*u^13 + Y*u^14 + u^15 + X^2*u^12 + u^13 + X*u^11 + Y*u^11
    + X^2*Y*u^8 + Y*u^9 + u^10 + X*Y*u^7 + X*u^8 + X*u^7 + X*u^6 + Y*u^6
    + X^2*Y*u^3 + X*Y*u^4 + X^2*Y*u^2 + u^5 + X^2*u^2 + X*u^3 + X^2*u + X*Y*u
    + X^2)/(X^2*u^9 + X*Y*u^8 + Y*u^9 + X*u^8 + X^2*Y + X*u);

P3<h3>:=PolynomialRing(K);

F3<h3>:=ext<K|h3^((q^2+1)*(q+1))-h33>;

P2<h2>:=PolynomialRing(F3);

F2<h2>:=ext<F3|h2 + ((X^2*Y + X^2)*u^3 + (X*Y + X^2)*u^2 + X*u + X^2*Y)/(u^3
```

```
    + Y*u^2 + (X*Y + 1)*u + (X*Y + X))*h3^3>;

h1 := (X*Y*u^4 + (X*Y + 1)*u + X^2*Y)/(u^7 + Y*u^6 + (X*Y + 1)*u^5 + (X*Y +
        X)*u^4 + (Y + X)*u^3 + u^2 + Y*u + (X*Y + 1))*h3^7;
g3 := X*Y*h3;
g2 := (X*Y + X)*h3^3;
g1 := (Y + 1)*h1 + (Y + X)*h2^2*h3 + (X*Y + 1)*h2*h3^4 + h3^7;
g0 := (X^2*Y + 1)*h1^2*h3 + (X*Y + X)*h1*h3^8 + (X^2*Y + X)*h2^5 + (X^2*Y +
        X)*h2^4*h3^3 + (X*Y + 1)*h2^2*h3^9 + X*h2*h3^12 + Y*h3^15 + Y + X^2;
    // =X^2
P1<a>:=RationalFunctionField(F2);
F1<tau>:=TwistedPolynomials(P1);
h0:=1; //normalized
phiX:=F1![X,g3,g2,g1,g0];
phiY:=F1![Y,h3,h2,h1,h0];
/*
choose <X,Y>-isogeny lambda of degree one.
Then lambda divides both phiX and phiY
*/
lambda:=F1![-a,1];
quX,re:=Quotrem(GCD(phiX,phiY),lambda);
Eltseq(re);
Eltseq(lambda*phiY);
Eltseq(phiY*lambda);
/*
[
    a^3 + ((X^2*Y + X^2)*u^8 + (X*Y + 1)*u^7 + (X^2*Y + X^2)*u^6 + (X^2*Y +
        1)*u^5 + u^4 + X*Y*u^3 + (Y + X^2)*u^2 + (X*Y + X)*u + (X^2*Y +
        X^2))/(u^13 + Y*u^12 + (Y + X)*u^9 + u^8 + (X*Y + X)*u^5 + (Y + X)*u^4 +
        (X*Y + 1)*u + (X*Y + X))*h3^13*a + (X*Y*u^7 + (Y + X^2)*u^6 + (X*Y +
        X)*u^5 + (X*Y + X^2)*u^4 + X^2*u^3 + Y*u^2 + (X^2*Y + X)*u + (Y +
        1))/(u^12 + (Y + X)*u^8 + (X*Y + X)*u^4 + (X*Y + 1))*h3^12
]
[
    Y*a,
    h3*a + X*Y + 1,
    ((X^2*Y + X^2)*u^3 + (X*Y + X^2)*u^2 + X*u + X^2*Y)/(u^3 + Y*u^2 + (X*Y +
        1)*u + (X*Y + X))*h3^3*a + h3^2,
    (X*Y*u^4 + (X*Y + 1)*u + X^2*Y)/(u^7 + Y*u^6 + (X*Y + 1)*u^5 + (X*Y + X)*u^4
        + (Y + X)*u^3 + u^2 + Y*u + (X*Y + 1))*h3^7*a + (X^2*Y*u^6 + (Y + 1)*u^4
        + X^2*u^2 + (X^2*Y + X))/(u^6 + (X*Y + 1)*u^4 + (Y + X)*u^2 + Y)*h3^6,
    a + ((Y + X^2)*u^8 + (Y + X)*u^2 + (X^2*Y + X))/(u^14 + (X*Y + 1)*u^12 + (Y
        + X)*u^10 + Y*u^8 + (X*Y + X)*u^6 + u^4 + (X*Y + 1)*u^2 + (Y +
        X))*h3^14,
    1
]
[
    Y*a,
    h3*a^2 + Y,
    ((X^2*Y + X^2)*u^3 + (X*Y + X^2)*u^2 + X*u + X^2*Y)/(u^3 + Y*u^2 + (X*Y +
        1)*u + (X*Y + X))*h3^3*a^4 + h3,
    (X*Y*u^4 + (X*Y + 1)*u + X^2*Y)/(u^7 + Y*u^6 + (X*Y + 1)*u^5 + (X*Y + X)*u^4
        + (Y + X)*u^3 + u^2 + Y*u + (X*Y + 1))*h3^7*a^8 + ((X^2*Y + X^2)*u^3 +
        (X*Y + X^2)*u^2 + X*u + X^2*Y)/(u^3 + Y*u^2 + (X*Y + 1)*u + (X*Y +
        X))*h3^3,
```

```
    a^16 + (X*Y*u^4 + (X*Y + 1)*u + X^2*Y)/(u^7 + Y*u^6 + (X*Y + 1)*u^5 + (X*Y +
        X)*u^4 + (Y + X)*u^3 + u^2 + Y*u + (X*Y + 1))*h3^7,
    1
]
*/


q:=2;
FX<X>:=GF(q,2);
P<Y>:=PolynomialRing(FX);
f:=Y^2 + X*Y + X^2 - X;

C<Y>:=ext<FX|f>;

K<v>:=RationalFunctionField(C);
/*
F(t22,t33)=F(v)
*/

t33:=(X*Y*v^13 + X*v^14 + Y*v^14 + v^15 + X*Y*v^12 + X*v^13 + Y*v^11 + v^12
    + X*Y*v^8 + X*v^9 + Y*v^9 + v^10 + X*Y*v^7 + X*v^8 + Y*v^6 + v^7
    + X*Y*v^3 + X*v^4 + Y*v^4 + v^5 + X*Y*v^2 + X*v^3 + Y*v + v^2 + 1)/
    (X^2*Y*v^8 + Y*v^9 + X*v^8 + v^9 + X^2*Y + v + 1);

t22 := (X*Y*v^13 + X*v^14 + Y*v^14 + v^15 + X^2*v^12 + X*v^13 + Y*v^12
    + Y*v^11 + X*v^9 + Y*v^9 + v^10 + X*Y*v^7 + Y*v^8 + v^8 + X^2*Y*v^4
    + Y*v^6 + v^7 + v^5 + X^2*Y*v + X^2*v^2 + Y*v^3 + v^4 + Y*v^2 + v^3
    + X)/(X^2*Y*v^9 + X^2*v^9 + X*Y*v^8 + v^8 + X^2*v + X^2 + X*Y);
P3<t3>:=PolynomialRing(K);

F3<t3>:=ext<K|t3^((q^2+1)*(q+1))-t33>;
P2<t2>:=PolynomialRing(F3);
F2<t2>:=ext<F3|t2 + ((Y + 1)*v^3 + (Y + X^2)*v^2 + X^2*Y*v + X)/(v^3
    + (Y + X)*v^2 + (X*Y + X)*v + (X*Y + 1))*t3^3>;

t1 := ((X*Y + X)*v^4 + (X^2*Y + X)*v + (X*Y + 1))/(v^7 + (Y + X)*v^6 + (X*Y
        + X)*v^5 + (X*Y + 1)*v^4 + Y*v^3 + v^2 + (Y + X)*v + (X*Y + X))*t3^7;
l3 := X*Y*t3;
l2 := (X*Y + X)*t3^3;
l1 := (Y + 1)*t1 + (Y + X)*t2^2*t3 + (X*Y + 1)*t2*t3^4 + t3^7;

l0 := (X^2*Y + 1)*t1^2*t3 + (X*Y + X)*t1*t3^8 + (X^2*Y + X)*t2^5 + (X^2*Y +
        X)*t2^4*t3^3 + (X*Y + 1)*t2^2*t3^9 + X*t2*t3^12 + Y*t3^15 + Y + X^2;
    // =X

P1<a>:=RationalFunctionField(F2);
F1<tau>:=TwistedPolynomials(P1);
t0:=1; //normalized
psiX:=F1![X,l3,l2,l1,l0];
psiY:=F1![Y,t3,t2,t1,t0];
lambda:=F1![-a,1];
quX,re:=Quotrem(GCD(psiX,psiY),lambda);
Eltseq(re);
Eltseq(psiY*lambda);
Eltseq(lambda*psiY);
```

```
/*
[
    a^3 + ((X*Y + X)*v^8 + (X*Y + X^2)*v^7 + (X*Y + X)*v^6 + (Y + X^2)*v^5 +
        X*Y*v^4 + v^3 + (X^2*Y + 1)*v^2 + (X^2*Y + X^2)*v + (X*Y + X^2))/(v^13 +
        (Y + X)*v^12 + Y*v^9 + v^8 + (X*Y + 1)*v^5 + Y*v^4 + (X*Y + X)*v + (X*Y
        + 1))*t3^13*a + ((X*Y + X)*v^7 + (Y + X^2)*v^6 + X*Y*v^5 + v^4 + (X^2*Y
        + 1)*v^3 + (X^2*Y + X^2)*v^2 + (X*Y + 1)*v + X^2*Y)/(v^12 + Y*v^8 + (X*Y
        + 1)*v^4 + (X*Y + X))*t3^12
]
[
    Y*a,
    t3*a^2 + Y,
    ((Y + 1)*v^3 + (Y + X^2)*v^2 + X^2*Y*v + X)/(v^3 + (Y + X)*v^2 + (X*Y + X)*v
        + (X*Y + 1))*t3^3*a^4 + t3,
    ((X*Y + X)*v^4 + (X^2*Y + X)*v + (X*Y + 1))/(v^7 + (Y + X)*v^6 + (X*Y +
        X)*v^5 + (X*Y + 1)*v^4 + Y*v^3 + v^2 + (Y + X)*v + (X*Y + X))*t3^7*a^8 +
        ((Y + 1)*v^3 + (Y + X^2)*v^2 + X^2*Y*v + X)/(v^3 + (Y + X)*v^2 + (X*Y +
        X)*v + (X*Y + 1))*t3^3,
    a^16 + ((X*Y + X)*v^4 + (X^2*Y + X)*v + (X*Y + 1))/(v^7 + (Y + X)*v^6 + (X*Y
        + X)*v^5 + (X*Y + 1)*v^4 + Y*v^3 + v^2 + (Y + X)*v + (X*Y + X))*t3^7,
    1
]

[
    Y*a,
    t3*a + X*Y + 1,
    ((Y + 1)*v^3 + (Y + X^2)*v^2 + X^2*Y*v + X)/(v^3 + (Y + X)*v^2 + (X*Y + X)*v
        + (X*Y + 1))*t3^3*a + t3^2,
    ((X*Y + X)*v^4 + (X^2*Y + X)*v + (X*Y + 1))/(v^7 + (Y + X)*v^6 + (X*Y +
        X)*v^5 + (X*Y + 1)*v^4 + Y*v^3 + v^2 + (Y + X)*v + (X*Y + X))*t3^7*a +
        (X*Y*v^6 + (X*Y + X^2)*v^4 + (X^2*Y + X)*v^2 + X^2)/(v^6 + (X*Y + X)*v^4
        + Y*v^2 + (Y + X))*t3^6,
    a + (Y*v^8 + (X^2*Y + 1)*v^2 + (Y + X))/(v^14 + (X*Y + X)*v^12 + Y*v^10 + (Y
        + X)*v^8 + (X*Y + 1)*v^6 + v^4 + (X*Y + X)*v^2 + Y)*t3^14,
    1
]
*/
```

6. Solving isogenous relations to find the tower equation $\Phi^1(u, v)$.

```
/* 6_x01_p.txt */
q:=2;
FX<X>:=GF(q,2);
P<Y>:=PolynomialRing(FX);
f:=Y^2 + X*Y + X^2 - X;

C<Y>:=ext<FX|f>;
K<u,v>:=RationalFunctionField(C,2);

F<a,h3,t3>:=PolynomialRing(K,3);

/*
lambda divides GCD(phiX,phiY) and lambda*phi = psi*lambda
*/
```

```
L:=[
    a^3 + ((X^2*Y + X^2)*u^8 + (X*Y + 1)*u^7 + (X^2*Y + X^2)*u^6 + (X^2*Y +
        1)*u^5 + u^4 + X*Y*u^3 + (Y + X^2)*u^2 + (X*Y + X)*u + (X^2*Y +
        X^2))/(u^13 + Y*u^12 + (Y + X)*u^9 + u^8 + (X*Y + X)*u^5 + (Y + X)*u^4 +
        (X*Y + 1)*u + (X*Y + X))*h3^13*a + (X*Y*u^7 + (Y + X^2)*u^6 + (X*Y +
        X)*u^5 + (X*Y + X^2)*u^4 + X^2*u^3 + Y*u^2 + (X^2*Y + X)*u + (Y +
        1))/(u^12 + (Y + X)*u^8 + (X*Y + X)*u^4 + (X*Y + 1))*h3^12,

    h3*a + X*Y + 1 - (t3*a^2 + Y),
   ((X^2*Y + X^2)*u^3 + (X*Y + X^2)*u^2 + X*u + X^2*Y)/(u^3 + Y*u^2 + (X*Y + 1)*u
        + (X*Y + X))*h3^3*a + h3^2 - (((Y + 1)*v^3 + (Y + X^2)*v^2 + X^2*Y*v
        + X)/(v^3 + (Y + X)*v^2 + (X*Y + X)*v + (X*Y + 1))*t3^3*a^4 + t3)
];
I:=ideal<F|L>;
B:=GroebnerBasis(I);

Write("Buv.txt",B);

/*
we can see that the last one of B is in t3, u, v. More precisely, in t3^15.
*/

t33:=(X*Y*v^13 + X*v^14 + Y*v^14 + v^15 + X*Y*v^12 + X*v^13 + Y*v^11 + v^12
    + X*Y*v^8 + X*v^9 + Y*v^9 + v^10 + X*Y*v^7 + X*v^8 + Y*v^6 + v^7 + X*Y*v^3
    + X*v^4 + Y*v^4 + v^5 + X*Y*v^2 + X*v^3 + Y*v + v^2 + 1)/(X^2*Y*v^8
    + Y*v^9 + X*v^8 + v^9 + X^2*Y + v + 1);
/*
let
g:=the last element of B in terms of t33, u and v;
it is a rational function in u,v
*/
Factorization(Numerator(g));
/*
[
    <v + Y + X, 45>,
    <u^3*v^2 + (X^2*Y + X^2)*u^3 + (Y + X^2)*u^2*v^2 + (X^2*Y + 1)*u^2*v + u^2 +
        Y*u*v^3 + (X^2*Y + X)*u*v^2 + Y*u*v + (X*Y + X)*u + (X^2*Y + X)*v^3 +
        Y*v^2 + (X^2*Y + 1)*v + X^2*Y + X, 1>,
    <u^75*v^58 + (X*Y + X^2)*u^75*v^57 + (Y + 1)*u^75*v^56 + (X*Y + 1)*u^75*v^55
        + X^2*Y*u^75*v^54 + u^75*v^53 + (X*Y + X^2)*u^75*v^52 + (Y +
        ...
]
The tower equation is the second one
*/
```

The same procedure applies for solving isogenous relations to find the tower equation $\Phi^2(v, w)$ by replacing component t_{33} by h_{33}.

Notations

$(x = \alpha)$	the zero of $x - \alpha$, page 11
$\deg \mathfrak{n}$	the degree of an ideal $\mathfrak{n}$ of a ring, page 19
δ	the degree of the fixed place ∞, page 19
∞	the fixed place of a function field, page 19
$\lambda(\mathcal{F})$	the limit of the tower $\mathcal{F}$, page 13
$\mathbb{P}_F$	the set of places of the function field F, page 10
$\phi[\mathfrak{n}]$	the set of $\mathfrak{n}$-torsion points of Drinfeld module ϕ, page 20
$\Phi_N(X, Y)$	Drinfeld modular polynomial, page 27
$\mathrm{Ram}(\mathcal{F}/F_j)$	the ramification locus of a tower $\mathcal{F}$ over one of its function field F_j, page 14
$\mathrm{Split}(\mathcal{F}/F_j)$	the splitting locus of a tower $\mathcal{F}$ over one of its function field F_j, page 14
A	the ring of functions of a function field F regular outside a fixed place ∞, page 19
$A(q)$	Ihara's constant, page 2
F_P	the residue class field of a place P, page 10

$L\{\tau\}$	the non-commutative polynomial ring generated by the Frobenius endomorphism, page 19
$N(C)$	the number of rational places of C, page 2
$x_0(\mathfrak{n})$	an absolutely irreducible component of Drinfeld modular curve $X_0(\mathfrak{n})$, page 48
$X_0(\mathfrak{n}), X_0(N)$	(projective) Drinfeld modular curve, page 22
$Y_0(\mathfrak{n}), Y_0(N)$	(affine) Drinfeld modular curve, page 21

Bibliography

[ABNed] N. Anbar, P. Beelen and N. Nguyen, The exact limit of some cubic towers, in *Arithmetic, geometry, cryptography and coding theory (AGCT 2015)*, submitted.

[Bae92] S. Bae, *On the modular equation for Drinfeld modules of rank* 2, J. Number Theory **42**(2), 123–133 (1992).

[BB05] P. Beelen and I. I. Bouw, *Asymptotically good towers and differential equations*, Compos. Math. **141**(6), 1405–1424 (2005).

[BB10] A. Bassa and P. Beelen, *The Hasse-Witt invariant in some towers of function fields over finite fields*, Bulletin of the Brazilian Mathematical Society, New Series **41**(4), 567–582 (2010).

[BB12] A. Bassa and P. Beelen, *A closed-form expression for the Drinfeld modular polynomial* $\Phi_T(X, Y)$, Arch. Math. (Basel) **99**(3), 237–245 (2012).

[BBGS15] A. Bassa, P. Beelen, A. Garcia and H. Stichtenoth, *Towers of function fields over non-prime finite fields*, Moscow Mathematical Journal **15**(1), 1–29 (2015).

[BBN14] A. Bassa, P. Beelen and N. Nguyen, Good towers of function fields, in *Algebraic curves and finite fields*, volume 16 of *Radon Ser. Comput. Appl. Math.*, pages 23–40, De Gruyter, Berlin, 2014.

[BBN15] A. Bassa, P. Beelen and N. Nguyen, *Good families of Drinfeld modular curves*, LMS Journal of Computation and Mathematics **18**, 699–712 (2015).

[BCH+99] B. C. Berndt, H. H. Chan, S.-S. Huang, S.-Y. Kang, J. Sohn and S. H. Son, *The Rogers-Ramanujan continued fraction*, J. Comput. Appl. Math. **105**(1-2), 9–24 (1999), Continued fractions and geometric function theory (CONFUN) (Trondheim, 1997).

[BCP97] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24**(3-4), 235–265 (1997), Computational algebra and number theory (London, 1993).

[Bee04] P. Beelen, *Graphs and recursively defined towers of function fields*, Journal of Number Theory **108**(2), 217–240 (2004).

[BG04] J. Bezerra and A. Garcia, *A tower with non-Galois steps which attains the Drinfeld-Vladut bound*, J. Number Theory **106**(1), 142–154 (2004).

[BGS05a] P. Beelen, A. Garcia and H. Stichtenoth, On towers of function fields over finite fields, in *Arithmetic, geometry, cryptography and coding theory (AGCT 2003)*, volume 11 of *Sémin. Congr.*, pages 1–20, Soc. Math. France, Paris, 2005.

[BGS05b] J. Bezerra, A. Garcia and H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound*, Journal für die reine und angewandte Mathematik **589**, 159–199 (2005).

[BGS08] A. Bassa, A. Garcia and H. Stichtenoth, *A new tower over cubic finite fields*, Moscow Mathematical Journal **8**(3), 401–418 (2008).

[CCX14] I. Cascudo, R. Cramer and C. Xing, *Torsion limits and Riemann-Roch systems for function fields and applications*, IEEE Transactions on Information Theory **60**(7), 3871–3888 (2014).

[CG12] N. Caro and A. Garcia, *On a tower of Ihara and its limit*, Acta Arithmetica **151**(2), 191–200 (2012).

[Dri74] V. G. Drinfeld, *Elliptic modules*, Mat. Sb. (N.S.) **94(136)**, 594–627, 656 (1974).

[Dri77] V. G. Drinfeld, *Elliptic modules. II*, Mat. Sb. (N.S.) **102(144)**(2), 182–194, 325 (1977).

[Elk98] N. D. Elkies, Explicit modular towers, in *Proceedings of the Thirty-Fifth [1997] Annual Allerton Conference on Communication, Control and Computing*, pages 23–32, Univ. of Illinois at Urbana-Champaign, 1998.

[Elk01] N. D. Elkies, Explicit towers of Drinfeld modular curves, in *European Congress of Mathematics, Vol. II (Barcelona, 2000)*, volume 202 of *Progr. Math.*, pages 189–198, Birkhäuser, Basel, 2001.

[Ful] W. Fulton, *Algebraic curves: an introduction to algebraic geometry*, free edition.

[Gek79] E.-U. Gekeler, *Drinfeld-Moduln und modulare Formen über rationalen Funktionenkörpern*, Bonner mathematische Schriften, Mathematischen Institut der Universität Bonn, 1979.

[Gek86] E.-U. Gekeler, *Drinfeld modular curves*, volume 1231 of *Lecture Notes in Mathematics*, Springer-Verlag, Berlin, 1986.

[Gek90] E.-U. Gekeler, *Sur la géométrie de certaines algèbres de quaternions*, Journal de théorie des nombres de Bordeaux **1**, 143–153 (1990).

[Gek04] E.-U. Gekeler, Asymptotically optimal towers of curves over finite fields, in *Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000)*, pages 325–336, Springer, Berlin, 2004.

[Gol03] D. M. Goldschmidt, *Algebraic functions and projective curves*, volume 215 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 2003.

[Gop81] V. D. Goppa, *Codes on algebraic curves*, Soviet Math. Dokl. **24**(1), 170–172 (1981).

[Gos96] D. Goss, *Basic structures of function field arithmetic*, volume 35 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*, Springer-Verlag, Berlin, 1996.

[GS95] A. Garcia and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfel′d-Vlăduţ bound*, Invent. Math. **121**(1), 211–222 (1995).

[GS96a] A. Garcia and H. Stichtenoth, *Asymptotically good towers of function fields over finite fields*, C. R. Acad. Sci. Paris Sér. I Math. **322**(11), 1067–1070 (1996).

[GS96b] A. Garcia and H. Stichtenoth, *On the asymptotic behaviour of some towers of function fields over finite fields*, J. Number Theory **61**(2), 248–273 (1996).

[GS05] A. Garcia and H. Stichtenoth, *Some Artin-Schreier towers are easy*, Mosc. Math. J. **5**(4), 767–774, 972 (2005).

[GS07] A. Garcia and H. Stichtenoth, Explicit towers of function fields over finite fields, in *Topics in geometry, coding theory and cryptography*, volume 6 of *Algebr. Appl.*, pages 1–58, Springer, Dordrecht, 2007.

[GSR03] A. Garcia, H. Stichtenoth and H.-G. Rück, *On tame towers over finite fields*, J. Reine Angew. Math. **557**, 53–80 (2003).

[GST97] A. Garcia, H. Stichtenoth and M. Thomas, *On towers and composita of towers of function fields over finite fields*, Finite Fields Appl. **3**(3), 257–274 (1997).

[Iha79] Y. Ihara, *Congruence relations and Shimūra curves. II*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **25**(3), 301–361 (1979).

[Iha81] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28**(3), 721–724 (1982) (1981).

[Iha07] Y. Ihara, Some remarks on the BGS tower over finite cubic fields, in *Proceedings of the conference "Arithmetic Geometry, Related Area and Applications" (Chuo University, April 2006)*, pages 127–131, 2007.

[LÖ7] E. C. Lötter, *On towers of function fields over finite fields*, PhD thesis, University of Stellenbosch, 2007.

[LMSE02] W.-C. W. Li, H. Maharaj, H. Stichtenoth and N. D. Elkies, New optimal tame towers of function fields over small finite fields, in *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 372–389, Springer, Berlin, 2002.

[man] Table of Curves with Many Points, `http://www.manypoints.org/`.

[MW05] H. Maharaj and J. Wulftange, *On the construction of tame towers over finite fields*, J. Pure Appl. Algebra **199**(1-3), 197–218 (2005).

[NX01] H. Niederreiter and C. Xing, *Rational points on curves over finite fields: theory and applications*, volume 285 of *London Mathematical Society Lecture Note Series*, Cambridge University Press, Cambridge, 2001.

[Ros02] M. Rosen, *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 2002.

[Sch95] A. Schweizer, *On the Drinfeld modular polynomial* $\Phi_T(X, Y)$, J. Number Theory **52**(1), 53–68 (1995).

[Sch97] A. Schweizer, Hyperelliptic Drinfeld modular curves, in *Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996)*, pages 330–343, World Sci. Publ., River Edge, NJ, 1997.

[Sch02] A. Schweizer, *On Drinfeld modular curves with many rational points over finite fields*, Finite Fields Appl. **8**(4), 434–443 (2002).

[Ser83] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris Sér. I Math. **296**(9), 397–402 (1983).

[Sti09] H. Stichtenoth, *Algebraic function fields and codes*, Springer, 2009.

[Tae06] L. Taelman, *Drinfeld modular curves have many points*, ArXiv Mathematics e-prints (February 2006), math/0602157.

[TVZ82] M. A. Tsfasman, S. G. Vladut and T. Zink, *Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound*, Math. Nachr. **109**, 21–28 (1982).

[VD83] S. G. Vladut and V. G. Drinfeld, *The number of points of an algebraic curve*, Funktsional. Anal. i Prilozhen. **17**(1), 68–69 (1983).

[vdGvdV02] G. van der Geer and M. van der Vlugt, *An asymptotically good tower of curves over the field with eight elements*, Bulletin of the London Mathematical Society **34**, 291–300 (5 2002).

[Zin85] T. Zink, Degeneration of Shimura surfaces and a problem in coding theory, in *Fundamentals of Computation Theory*, edited by L. Budach, volume 199 of *Lecture Notes in Computer Science*, pages 503–511, Springer Berlin Heidelberg, 1985.

Index